Facultad de Ingeniería

Carrera de Ingeniería de Seguridad y Auditoría Informática

TRABAJO DE INVESTIGACIÓN PARA OPTAR POR EL GRADO ACADÉMICO DE BACHILLER EN INGENIERÍA DE SEGURIDAD Y AUDITORÍA INFORMÁTICA

Diseño de un Sistema de Gestión de Continuidad de Negocio basado en la ISO 22301 para la empresa Desarrollo A1

Autores

Vargas Barrios, Pedro Javier (1412925)

Velazquez Romero, Sebastian Alonso (1610599)

Asesores

Rodríguez Vilcamore, Carlos Daniel

Rojas Nieves, Luis Alfonso

Lima, Perú

Diciembre, 2020

Contenido

Índice de Tablas

6. Tabla 6. Matriz de costos (Creación propia)

1. Resumen

El presente documento sustenta la propuesta de la elaboración del diseño de un sistema de continuidad del negocio para pequeñas empresas y proponer una estructura base para que toda pequeña empresa del rubro de desarrollo y consultoría de software lo pueda adoptar.

Este proyecto surge de la necesidad de toda empresa de contar con un sistema de gestión de continuidad del negocio. Sin embargo, el contar con dicho sistema demanda una inversión, tiempo y esfuerzos que pequeñas empresas no pueden asumir.

Como resultado final, se elaboró un diseño sobre una empresa ficticia, Desarrollos A1, que cuenta con las consideraciones necesarias para que se pueda disponer de un sistema de gestión de continuidad del negocio sólido y alineado a las capacidades de la empresa para que puedan recuperarse frente a cualquier incidente que interrumpa sus servicios.

2. Palabras Clave

Continuidad del negocio, continuidad operativa, servicios críticos, interrupción, análisis de riesgos, análisis de impacto en el negocio, BIA, estrategias de continuidad de operaciones, estrategia de respuestas a riesgos.

3. Problema de Investigación

3.1. Problema

En cualquier organización, siempre existen riesgos los cuales pueden poner en peligro el funcionamiento y la continuidad de sus operaciones. El 80% de las empresas en el mundo en algún momento sufrieron de problemas de continuidad de negocio debido a cortes de energía, fallas en sistemas de TI, desastres naturales, etc. (BSI, 2016)

En la actualidad las organizaciones están afrontando una situación de crisis debido al COVID-19. Esta pandemia ha creado la necesidad de cambiar el modelo de negocio de las empresas con el fin de adaptarse a las nuevas medidas establecidas para reincorporarse a su sector correspondiente.

Las empresas del rubro de consultoría y desarrollo de TI, también se vieron afectadas debido a la falta o mal establecimiento de un plan de gestión de riesgos y de continuidad del negocio, esto deriva en pérdidas económicas, pérdida de clientes, incumplimiento de contratos, poca o nula fiabilidad de la calidad del proyecto, etc.

3.2. Pregunta de Investigación

¿De qué manera el diseño de un Sistema de Gestión de Continuidad del Negocio basado en la norma ISO 22301 ayuda a la recuperación de las actividades del negocio y mantener el riesgo en niveles aceptables frente a un incidente o interrupción?

4. Objetivos

4.1. Objetivo General

Diseñar un Sistema de Gestión de la Continuidad del Negocio basado en la norma ISO 22301 para la rápida recuperación o el mantenimiento a un nivel aceptable de las actividades críticas del negocio frente a un incidente o interrupción.

4.2. Objetivos Específicos

- Entender a la organización y sus necesidades para establecer el contexto en el que se aplicara el Sistema de Gestión de Continuidad del Negocio.
- Analizar las acciones a tomar para cubrir riesgos y oportunidades para el diseño del plan de continuidad en los procesos del Sistema de Gestión de Continuidad del Negocio.
- Evaluar la eficacia de las acciones propuestas en el análisis de los riesgos del Sistema de Gestión de Continuidad del Negocio.

5. Justificación de la Investigación

La continuidad de negocio es de suma importancia en empresas del rubro de consultoría y desarrollo de software, debido a la necesidad de poder mantener los servicios operativos dentro de niveles aceptables, en especial en nuestro país, que a inicios de cada año siempre se presentan fenómenos naturales. Así mismo, el SGCN disminuye las pérdidas financieras de la empresa debido a que, ayuda a gestionar de mejorar manera los riesgos, la probabilidad e impacto de estos y la posibilidad de sufrir sanciones económicas por incumplimiento de contratos y leyes.

6. Marco teórico

Con el fin de describir las fases sobre las cuales se basa la norma ISO 22301, se detallarán las que se desarrollarán en la metodología y que satisfacen la solución al problema planteado. Esta descripción permitirá determinar las cláusulas específicas agrupadas en fases que se emplean en todo sistema de gestión.

6.1. Sistema de Gestión de la Continuidad del Negocio basado en la norma ISO 22301

Según (CertiProf, 2018, pág. 11), un Sistema de Gestión de la Continuidad del Negocio es parte del sistema global de gestión de una organización el cual establece, implanta, opera, supervisa, revisa, mantiene y mejora la continuidad del negocio. Este

permite a la organización controlar los riesgos, los efectos de estos y los controles que permiten a las empresas mantener sus servicios y operaciones en niveles aceptables frente a una interrupción de sus procesos. A continuación, se describirán las cláusulas que comprenden la norma ISO 22301.

6.1.1. Contexto de la organización

Según CertiProf 2018, en esta cláusula se documenta la organización, con el fin de conocer sus necesidades internas y externas, para establecer el alcance y el contexto del SGCN, así como las necesidades y requisitos.

6.1.2. Liderazgo

Brinda los requisitos específicos de la función y la relación de la alta dirección con el SGCN, la forma en la que se debe comunicar con la organización por medio de declaraciones políticas (CertiProf, 2018, pág. 27).

6.1.3. Planificación

Se definen los requisitos para el establecimiento de los objetivos estratégicos para el SGCN. En esta etapa, la organización debe planificar las acciones para tratar los riesgos y oportunidades, así como la manera de cómo se integrarán las acciones en los procesos del SGCN y cómo se evaluará la eficacia de estas acciones (CertiProf, 2018, pág. 28).

6.1.4. Soporte

Se basa en el apoyo a las operaciones de parte del personal con los conocimientos, experiencia y habilidades pertinentes para la implementación del SGCN. Se incluye aquí el establecimiento de las comunicaciones con las partes interesadas y gestión de la comunicación en caso de que ocurra un incidente (CertiProf, 2018, pág. 29).

6.1.5. Operación

En esta etapa la empresa u organización determina la manera de tratar y desarrollar los procedimientos para gestionar un incidente disruptivo. Por otro lado, se realizan evaluaciones de riesgos con el fin de tratarlos e informar de estos en el desarrollo del

SGCN, así como, la realización del análisis de impacto en el negocio, la implantación de los procedimientos para garantizar que el plan es coherente con los objetivos de la organización. (CertiProf, 2018, pág. 30)

6.1.6. Evaluación de rendimiento

Resume los requisitos necesarios para medir el rendimiento y la conformidad de la gestión de continuidad con la norma internacional y las expectativas de la dirección. (CertiProf, 2018, pág. 30)

6.2. Análisis de Impacto al Negocio (BIA)

En el análisis de impacto al negocio se tiene como principal objetivo identificar las necesidades del negocio en términos de recuperación. Se debe considera las catalogadas como indispensables o servicios críticos para el funcionamiento de la organización. Como resultado de los trabajos de análisis se dispondrá de un conjunto de procesos o actividades para los cuales se deben definir el MAO (Maximun Acepted Objective), RTO (Recovery Time Objective) y RPO (Recovery Point Objective). Con esta información se crea una lista ordenada por prioridad y obtener las actividades críticas para identificar cuáles son los activos críticos de TI.

Descripción			Impacto					
Proceso	Sub Proceso	Responsable	Económico	Operacional	Desarrollo de Marca	Legal	Resultados	¿Proceso Crítico?

1. Tabla 1. Matriz BIA (Creación propia)

6.3. Evaluación de riesgos

Para clasificar jerárquicamente los riesgos, primero se debe identificar el impacto que tenga mayor afectación en el contexto, después se debe definir la probabilidad con la que ocurrirán estos impactos. A continuación, la fórmula que se tendrá que emplear para la medición del riesgo.

Para la realización de la matriz, se debe ingresar la actividad que puede originar el riesgo. Seguidamente, definir y explicar las causas por las cuales el riesgo se podría llegar a materializar. Luego, se define el riesgo que fue identificado para identificar cuáles serían las consecuencias en caso se materialice el riesgo. A continuación, la plantilla de la matriz de probabilidad e impacto de los riesgos.

IDENTIFICACIÓN DE PELIGRO					EVALUACIÓN DE RIESGOS		
ÁREA	ACTIVIDAD	CAUSA	RIESGO	CONSECUENCIA	PROBABILIDAD	IMPACTO	RIESGO

2. Tabla 2. Matriz de Análisis de Riesgos (Creación propia)

Así mismo para poder definir la probabilidad de que un riesgo se materialice, se utilizarán cinco niveles de ocurrencia. A continuación, se mostrará la matriz de magnitud de probabilidad, la cual cuenta con una valorización, el nivel de la probabilidad y su respectiva descripción.

MAGNITUD DE PROBABILIDAD		
VALOR	PROBABILIDAD	DESCRIPCIÓN
1	Muy Bajo	
2	Bajo	
3	Medio	
4	Alto	
5	Crítico	

3. Tabla 3. Matriz Magnitud de Probabilidad (Creación propia)

Del mismo modo, para el impacto, se utilizará una matriz la cual define el impacto en cinco niveles de severidad, estos van desde el nivel muy bajo hasta crítico, siendo este un retraso de 3 días a más. A continuación, se mostrará la magnitud de impacto, la cual cuenta con una valorización, el nivel de impacto y su respectiva descripción.

MAGNITUD DE IMPACTO NEGATIVO

VALOR	IMPACTO	DESCRIPCIÓN
1	Muy Bajo	
2	Bajo	
3	Medio	
4	Alto	
5	Crítico	

4. Tabla 4. Matriz Magnitud de Impacto (Creación propia)

Para hallar el riesgo de una actividad, tomando en cuenta tanto la probabilidad por el impacto que un riesgo tendría en caso se materialice. Para esto se tendrá que tomar en cuenta la siguiente matriz de probabilidad e impacto.

PROBABILIDAD IMPACTO	Muy Bajo	Bajo	Medio	Alto	Crítico
Muy Bajo	1	2	3	4	5
Bajo	2	4	6	8	10
Medio	3	6	9	12	15
Alto	4	8	12	16	20
Crítico	5	10	15	20	25

5. Tabla 5. Matriz Magnitud de Probabilidad (Creación propia)

7. Estado del Arte

Actualmente la norma ISO 22301 es el estándar mundial que permite el diseño e implementación de la continuidad del negocio en las organizaciones. Sin embargo, esta norma no se creó desde la existencia del concepto de continuidad de negocio. A lo largo del tiempo, la evolución de este concepto ha dado paso al desarrollo de lineamientos, buenas prácticas y otros estándares.

En 1995 se creó el primer lineamiento para la gestión de desastres, emergencias y programas de continuidad, el NFPA 1600. En 1997, se publicaron las Prácticas Profesionales para la Gestión del Negocio por el Disaster Recovery Institute International (DRII). (CertiProf, 2018, pág. 14) Cinco años después, en el 2002, se definieron los lineamientos para las Buenas Prácticas para la Continuidad del Negocio por el Business Continuity Institute (BCI), para que, al año siguiente, con el PAS 56 se

empiece a establecer el proceso, principios y la terminología para el Sistema de Gestión de Continuidad del Negocio en base a los lineamientos definidos hasta el momento.

Desde el 2007, tras definir los lineamientos genéricos para que las organizaciones que deseen establecer un Sistema de Gestión se preparen ante cualquier incidente en la ISO/PAS 22399, se han ido estableciendo, mejorando y corrigiendo los códigos de buenas prácticas sobre Continuidad del negocio y todo lo relacionado a ello. (CertiProf, 2018, pág. 15)

Finalmente, en el 2011 se exponen los conceptos y principios de tecnología de información y comunicación (ICT) para preparar a una organización para la continuidad del negocio en la ISO/IEC 27031. Esto permitió que en el 2012 se establezca la primera norma certificable y auditable que reúne los conceptos principales de los lineamientos anteriores publicados desde 1995, la ISO 22301 para el diseño de Sistemas de Gestión de Continuidad del Negocio. (CertiProf, 2018, pág. 16)

Como se puede apreciar, la norma ISO 22301 es un estándar que se ha formado y perfeccionado desde 1995, la cual cuenta hoy en día, con respaldo y aprobación a nivel internacional, garantizando que toda organización que decida diseñar e implementar un plan de continuidad del negocio alcanzando la más alta eficacia y resiliencia en sus procesos, protegiendo su imagen corporativa y disminuyendo las pérdidas económicas.

Hoy en día en el Perú, pocas empresas de consultoría y desarrollo de software cuentan con la capacidad para responder ante cualquier interrupción en la continuidad de sus procesos, en especial las de pequeño tamaño. Debido al aumento latente de incidentes, el Sistema de Gestión de Continuidad del Negocio, se ha vuelto una necesidad para la mayoría de las empresas, con el objetivo principal de garantizar la continuidad operacional en sus procesos.

Gustavo Gonzáles (2017), desarrolló una investigación titulada “Plan de Continuidad del Negocio basado en servicios en la nube para el área de tecnología”. La investigación tuvo como principal objetivo conocer la sencillez del diseño e

implementación de un plan de continuidad. De este modo, presenta la factibilidad en su ejecución y puesta en marcha por medio de los servicios en la nube. Así mismo, resalta que al momento de diseñarlo es necesaria la coordinación con la alta dirección de la organización para recuperar las funciones críticas del negocio frente a una interrupción o desastre. Esto incluye los desastres a corto, mediano o largo plazo, incendios, inundaciones, terremotos, interrupciones de energía eléctrica e incidentes provocados por el hombre. (págs. 7 y 8)

Esta investigación, permite tener un enfoque de continuidad orientado al área informática de la organización, la cual es la encargada del desarrollo y gestión de los productos y servicios que se brindan dentro de una empresa que tiene como rubro la consultoría y desarrollo de software. Este modelo, le permitió diseñar un plan con las guías necesarias para cubrir desastres naturales, errores humanos o fallos tecnológicos, minimizando las consecuencias negativas y las pérdidas económicas en caso de presentarse eventos adversos como los mencionados con anterioridad. Todo plan que se vaya a diseñar debe estar debidamente contextualizado a la realidad de la empresa en la que se desarrollará.

De este modo, Gonzáles diseñó su plan de continuidad con cinco secciones. En primer lugar, la introducción, donde se describen los aspectos principales como los roles, responsabilidades y actividades. En segundo lugar, la estrategia de continuidad del negocio, donde se describe la estrategia para mantener la continuidad. En tercer lugar, los equipos de recuperación, donde se describe las funciones de los colaboradores clave en la recuperación de las operaciones. En cuarto lugar, los procedimientos de equipos, donde se describe el orden de las tareas y actividades a seguir, así como las personas involucradas. Finalmente, el apéndice, donde se visualizan los conceptos y definiciones abordadas en determinados puntos del plan. (pág. 12)

Del mismo modo, Laura Castro (2013), diseñó un modelo de Sistema de Gestión de Continuidad del Negocio, en el cual se evidencia, como parte del diseño, la necesidad de un análisis de riesgo, un análisis de impacto y un plan de manejo de crisis, de

emergencia, de recuperación de desastres, de continuidad del negocio y de pruebas. (págs. 9-10)

Una vez que se definió el modelo para diseñar el plan de continuidad del sistema de gestión, este debe contar con determinados entregables que sirvan de insumo para desarrollar una estrategia de continuidad orientada a lograr una adecuada y efectiva respuesta, la cual no será ajena a los objetivos del negocio. Por ello, es necesario entender, en una primera instancia, el contexto al que pertenece la organización, los objetivos y necesidades que deben cumplir, y los requerimientos de sus productos y servicios.

Por otra parte, Castro afirma que, “en el Perú, la continuidad de negocios no es un tema ajeno, […] la Norma Técnica Peruana 27001 [INDECOPI, 2008], incluye un dominio de continuidad de negocios, direccionado a empresas públicas para reducir las interrupciones a causa de factores internos o externos”. (págs. 4-5) Para ello se debe determinar los factores externos e internos relevantes para la elaboración del sistema de gestión, debido a que las organizaciones de todo tipo de tamaño y complejidad operan en circunstancias que están sujetas a oportunidades, cambios y riesgos. Consecuentemente, la organización evalúa dicha información para poder innovar, mantener y mejorar la efectividad de su sistema de gestión.

Cabe resaltar que la norma ISO 22301 es aplicable independientemente del rubro al cual pertenezca la organización. Eso se demuestra en la investigación elaborada en el 2019 por Anthony Rázuri, en donde al igual que el resto de las investigaciones, su objetivo es demostrar que el sistema de gestión permite a la organización estar preparada para hacer frente a situaciones adversas que pongan en riesgo el cumplimiento de sus objetivos, describiendo la importancia y beneficios que consigo trae su implementación. (pág. 7)

Como se puede inferir, el diseño de un sistema de gestión de continuidad de negocio, independientemente el tipo o tamaño de organización, ayuda a hacer uso de los

recursos de forma eficiente, disminuyendo costos e incrementando su productividad y resiliencia.

Toda empresa de consultoría y desarrollo de software debe garantizar la continua operatividad y resiliencia en sus soluciones. Además, como proveedor debe ofrecer la máxima calidad y confianza en el soporte de los productos y servicios que brinda. Sin embargo, existen eventualidades externas e internas que ocasionan la interrupción en los procesos o inclusive el cierre temporal o permanente de la empresa.

Hoy en día, debido a la época de crisis a causa del COVID-19, el foco de la estrategia de los planes de continuidad de negocio ha cambiado. Esto se ve plasmado en el artículo “Garantizar la continuidad de negocio ante el COVID-19” escrito por Álvaro Méndez. Por ello, cada vez que se definen los alcances del proyecto y riesgos actuales de la empresa, estos deben contemplar los empleados y de este modo poder proporcionar los recursos necesarios para que estos puedan trabajar desde sus hogares con laptops, conexiones VPN, telefonía móvil laboral, y para los que no puedan trabajar de sus hogar se les debe proporcionar medios alternativos y seguros bajo los lineamientos actuales de salud ocupacional. Además de estos recursos, el plan debe disponer de un comité que gestione esta situación de anormalidad como de los planes de comunicación reestructurados para mantener informados a los empleados, a los equipos que ejecutan las tareas de recuperación, y a todos los grupos de interesado. (Tejeda, 2020)

De acuerdo con una investigación mencionada en la conferencia de José Calderón (2014), Data Center & Security Country Head de la empresa Level 3, el 43% de las compañías que enfrentan una situación de desastre no vuelven a operar y el 29% cierra en dos años. Por otro lado, el 99% de las empresas que pierden servicios de centros de datos por 10 días se declaran en bancarrota en el lapso de un año. Finalmente, el 40% de las empresas que enfrentan una situación de desastre salen del mercado si no tienen acceso a su centro de datos en un lapso de 24 horas.

Particularmente en el Perú, pocas empresas cuentan con un Sistema de Gestión de Continuidad del Negocio, y más aún están certificadas en la norma ISO 22301. En el sector de consultoría y desarrollo de software, las pequeñas empresas no conforman parte del grupo empresarial acreditado en la norma. Esto se debe a que muchas de ellas no se encuentran en capacidades económicas de diseñar y establecer una. Sin embargo, de las pocas empresas certificadas en el sector se encuentra IBM desde el 2017, lo cual evidencia el factor diferenciador y de crecimiento económico de contar con un sistema de gestión que permita soportar la infraestructura tecnológica de la empresa. (Bureau Veritas, 2017)

Dado los hechos acontecidos a nivel nacional en diferentes sectores empresariales además de Claro, toda organización debe estar preparada ante cualquier interrupción o incidente de sus procesos frecuentes y críticos, de tal modo que garanticen una rápida recuperación, reduciendo el Tiempo Máximo Aceptable de Interrupción (TMAI) a un tiempo aceptable. Por ello, contar con un plan de continuidad normado y aprobado anualmente es de suma importancia, ya que diariamente surgen eventualidades no planeadas que afecten el normal funcionamiento de la organización.

8. Hipótesis

El proyecto no contempla una hipótesis, debido a que es de conocimiento general que la implementación de un SGCN basado en un estándar internacional traerá consecuencias positivas y facilitará el cumplimiento de los objetivos de la empresa. Por lo cual, este proyecto se enfocará en brindar el diseño de un SGCN con el fin de favorecer y agilizar el proceso de su implementación en empresas del rubro de consultoría y desarrollo de software.

9. Metodología

El presente trabajo de investigación será desarrollado en base al ciclo de Deming. Este propone dividir las cláusulas de la ISO 22301 en cuatro etapas, de las cuales las tres primeras son utilizadas para el diseño el SGCN. A continuación, se desarrollará las

etapas que abordan, con sus respectivas cláusulas y fases, únicamente el diseño e implementación del SGCN.

9.1. Etapa N° 1: Planear

En esta etapa se debe hacer la planificación del diseño e implementación de la gestión de continuidad del negocio. Así mismo, debe quedar establecido el alcance de la gestión, el cual debe formar parte del plan, y como mínimo, el plan debe incluir el alcance del sistema de gestión.

9.1.1. Cláusula N° 4: Contexto de la organización

9.1.1.1. Fase N° 1: Comprensión de la organización y su contexto

La organización establece, implanta y mantiene un procedimiento para la identificación y evaluación de los objetivos, factores involucrados y requisitos legales orientados a la continuidad del negocio. Así mismo, se deberá cerciorar de que estos se estén cumpliendo.

9.1.1.1.1. Actividad N°1: Realizar recolección de información

Realizar una recolección de documentos para asegurar el entendimiento del contexto de la empresa y garantizar la consistencia en la futura selección de estrategias para el SGCN.

Entregable: Documentos de la empresa relacionada a leyes, funciones, servicios y productos.

Herramientas: Microsoft Word

9.1.1.2. Fase N° 2: Determinación del alcance del SGCN

La organización deberá definir el alcance que tendrá el SGCN basándose en el punto 7.1.1.1 del presente proyecto de investigación para tenerlo en cuenta en la aplicabilidad del SGCN.

9.1.1.2.1. Actividad N° 2: Hacer las Reuniones y lluvia de ideas

Para llevar a cabo de manera correcta la lluvia ideas es necesaria la participación abierta de todos. El alcance se tendrá que identificar mediante una reunión, la cual será validada con un acta firmada por los involucrados.

Entregable: Acta de constitución

Herramientas: Microsoft Word

9.1.1.3. Fase N° 3: Determinación de los riesgos organizacionales

La organización deberá definir los riesgos que tiene la organización actualmente. Así mismo, deberán tener en cuenta los activos, factores internos y factores externos de la organización.

9.1.1.3.1. Actividad N° 3: Hacer las Reuniones y lluvia de ideas

Para llevar a cabo de manera correcta la lluvia ideas es necesaria la participación abierta de todos. Las actividades tendrán ser validadas con un acta firmada por los involucrados.

Entregable: Acta de reunión; Lista de riesgos potenciales

Herramientas: Microsoft Word

9.1.2. Cláusula N° 5: Liderazgo

9.1.2.1. Actividad N° 4: Asignación de roles y responsabilidades

La matriz de asignación de responsabilidad, o RACI, mapea tareas y las relaciona con los roles de los servicios y la toma de decisiones. Se debe determinar quién está involucrado en el proyecto con sus respectivas funciones.

Entregable: Matriz RACI

Herramientas: Microsoft Excel

9.1.3. Cláusula N° 7: Soporte

9.1.3.1. Actividad N° 5: Gestionar los recursos

La empresa tiene que determinar y proporcionar todos los recursos humanos y físicos necesarios. Los recursos proporcionados deben ser documentados y asignados a de acuerdo con los planes y roles definidos con anterioridad.

Entregable: Listado de recursos asignados; Cronograma de concientización.

Herramientas: Microsoft Excel

9.2. Etapa N° 2: Hacer

En esta etapa, se debe ejecutar las actividades necesarias para el diseño del sistema de la gestión de continuidad del negocio. Se debe incluir la asignación de presupuesto, funciones y responsabilidades, brindar la documentación de mantenimiento de políticas, procedimientos para la definición de cada proceso crítico que se abarcará en los análisis correspondientes. Esto con el fin de establecer los planes necesarios en base a las estrategias definidas para abordar los riesgos evaluados.

9.2.1. Cláusula N°6: Planificación

9.2.1.1. Fase N° 4: Acciones para Abordar los Riesgos y Oportunidades

Es necesario tener en cuenta los puntos 8.1.1.3 para considerar los riesgos y oportunidades que se tendrán que abordar con el fin de asegurar que el sistema de gestión pueda conseguir los resultados esperados.

9.2.1.1.1. Actividad N° 6: Analizar el Impacto al Negocio

En el análisis de impacto en el negocio se tiene como principal objetivo identificar las necesidades del negocio en términos de recuperación, para luego realizar el análisis e identificar los procesos críticos.
Entregable: Matriz de análisis de impacto al negocio

Herramientas: Pilar Basic; Microsoft Excel

9.2.1.1.2. Actividad N° 7: Evaluar los riesgos

Para la realización de la matriz, se debe ingresar la actividad que puede originar el riesgo. Seguido de la definición y explicación de las causas por las cuales el riesgo se podría llegar a materializar.

Entregable: Matriz de magnitud de probabilidad; Matriz de magnitud de impacto; Matriz de evaluación de riesgos; Mapa de calor

Herramientas: Pilar Basic; Microsoft Excel

9.2.1.2. Fase N° 5: Estrategias de Continuidad de Negocio

Se definen la estrategia de respuestas para los resultados obtenidos de la evaluación de riesgos y el BIA. Del mismo modo, estas estrategias deben incluir el tiempo que deben tomar aplicarlas y los niveles de priorización para la reanudación de las actividades.

9.2.1.2.1. Actividad N°8: Determinar y seleccionar las estrategias

Se determina y selecciona las estrategias en base al BIA y la evaluación de riesgos, para la protección, priorización, estabilización, reanudado y mitigación de riesgos.

Entregables: Matriz de Medidas de Control; Matriz de Medidas de Control Mejorada

Herramientas: Pilar Basic; Microsoft Excel

9.2.1.2.2. Actividad N°9: Establecer los requerimientos de recursos

Se establecen los recursos a utilizar en base a la información proporcionada tras el análisis de riesgos para disponer de los recursos necesarios en caso algún riesgo se materialice.

Entregables: Matriz de requerimiento de recursos.

Herramientas: Microsoft Excel

9.2.2. Cláusula N° 8: Operación

9.2.2.1. Fase N°6: Establecer Procedimientos de Continuidad de Negocio

La empresa debe documentar todos los procedimientos y planes propuestos para asegurar la continuidad de actividades y gestión de un incidente que genere interrupción.

9.2.2.1.1. Actividad N° 10: Establecer los planes para el SGCN

Se establecen los planes, en los cuales se encuentran los procedimientos para responder a interrupciones de las operaciones de diferentes niveles de criticidad.

Entregable: Plan de continuidad del Negocio (BCP); Plan de recuperación de Negocio (BRP); Plan de crisis de comunicaciones; Plan de recuperación de desastres (DRP)

Herramientas: Microsoft Word

9.3. Etapa N° 3: Verificar

En esta etapa, se tiene que supervisar y verificar todos los objetivos propuestos y el plan de gestión de continuidad del negocio establecido en la organización, para comprobar que se cumplen. La norma ISO 22301 indica que los resultados de la verificación deben ofrecer información que garantice que el programa de continuidad del negocio es efectivo

9.3.1. Cláusula N°9: Evaluación de Desempeño

9.3.1.1. Fase N°7: La medición, análisis y evaluación

La empresa debe retener la información adecuada y documentada como evidencia de los resultados de la evaluación del rendimiento y la eficacia del Sistema de Gestión de Continuidad del Negocio.

9.3.1.1.1. Actividad N°11: Realizar la auditoría interna

La empresa debe llevar a cabo auditorías internas, en intervalos planificados, con el fin de evaluar el nivel de cumplimiento de las medidas de control que están basadas en los requisitos del SGCN.

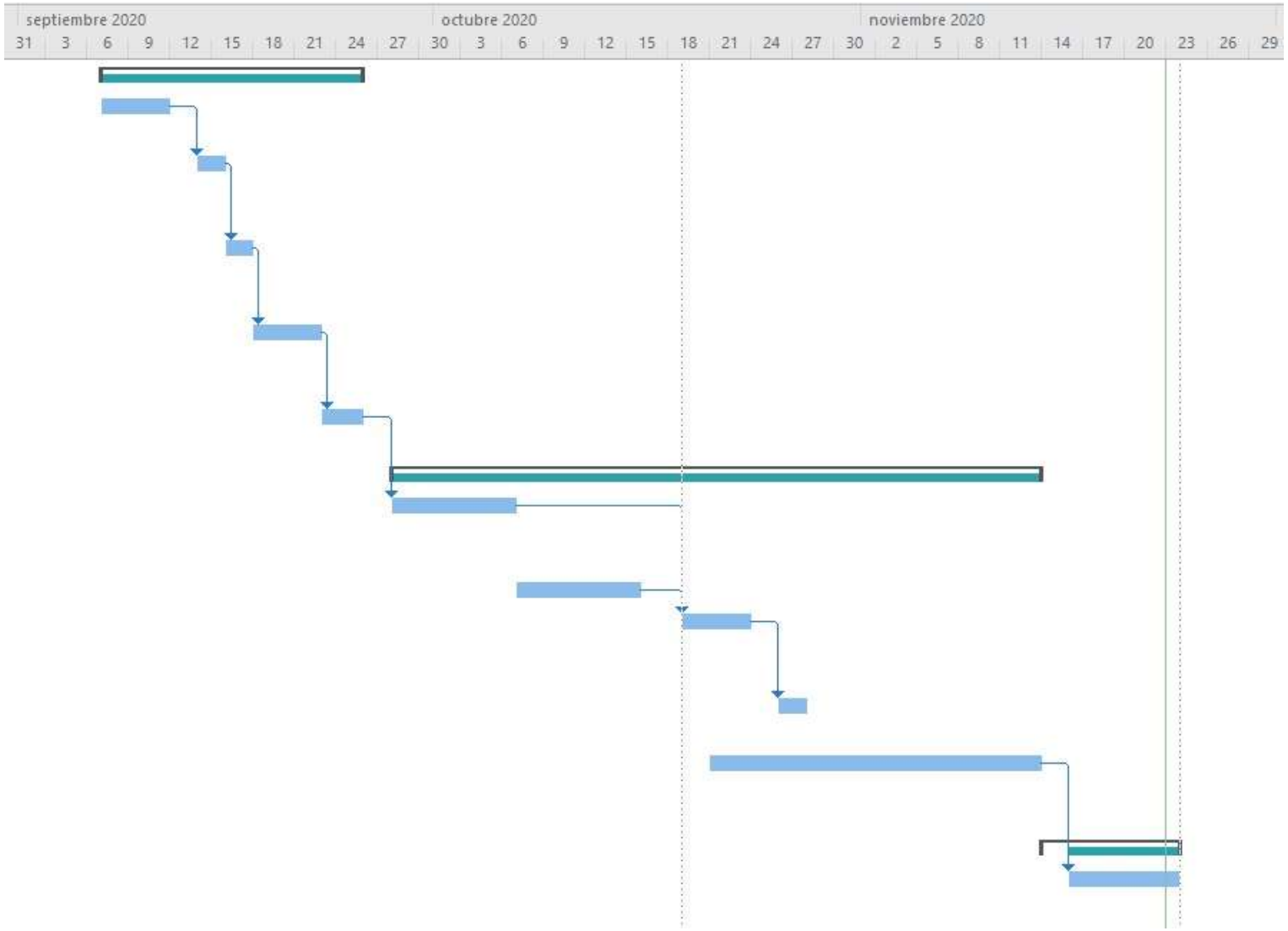
Entregables: Lista de cumplimiento (correspondiente al primer ciclo de Deming); Análisis GAP (correspondiente a todos los ciclos de Deming posteriores al primero)

9.3.1.2. Fase N°8: Revisión por la dirección

En esta revisión debe estar incluido el estado real de la organización que se realizó en la evaluación de riesgos y el nivel de cumplimiento de las medidas de control, información sobre el rendimiento, conformidades y acciones correctivas, oportunidades de mejora para la organización y la eficacia de los procedimientos descritos en los planes.

10. Cronograma de Actividades

	Modo de	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1		**Etapa 1 - Planear**	**15 días**	**lun 7/09/20**	**vie 25/09/20**	
2		Recolección de información	5 días	lun 7/09/20	vie 11/09/20	
3		Reunión para determinar el alcance del SGCN	2 días?	lun 14/09/20	mar 15/09/20	2
4		Reunión para determinar los riesgos	2 días?	mié 16/09/20	jue 17/09/20	3
5		Asignación de roles y responsabilidades	3 días?	vie 18/09/20	mar 22/09/20	4
6		Gestionar los recursos	3 días?	mié 23/09/20	vie 25/09/20	5
7		**Etapa 2 - Hacer**	**35 días**	**lun 28/09/20**	**vie 13/11/20**	
8		Análisis de impacto al negocio BIA	7 días	lun 28/09/20	mar 6/10/20	6
9		Evaluar los riesgos	7 días	mié 7/10/20	jue 15/10/20	
10		Determinar y seleccionar las estrategias	5 días	lun 19/10/20	vie 23/10/20	9;8
11		Establecer los recursos	2 días	lun 26/10/20	mar 27/10/20	10
12		Establecer los planes para el SGCN	18 días?	mié 21/10/20	vie 13/11/20	
13		**Etapa 3 - Verificar**	**7 días**	**sáb 14/11/20**	**lun 23/11/20**	
14		Realizar la auditoría interna	6 días?	lun 16/11/20	lun 23/11/20	12


septiembre 2020
octubre 2020
noviembre 2020
31 3 6 9 12 15 18 21 24 27 30 3 6 9 12 15 18 21 24 27 30 2 5 8 11 14 17 20 23 26 29

11. Presupuesto

Matriz de costos (16 semanas)				
Recursos humanos				**S/ 15,800.00**
Necesidad	Recurso	Horas	Costo	Total
Requerido	Implementador de SGCN	150	S/ 40.00	S/ 6,000.00
Opcional	Supervisor Operacional de Continuidad	140	S/ 50.00	S/ 7,000.00
Opcional	Miembro de equipo de desarrollo	70	S/ 20.00	S/ 1,400.00
Opcional	Miembro de equipo de desarrollo	70	S/ 20.00	S/ 1,400.00
Recursos tecnológicos				**S/ 5,600.00**
Necesidad	Recurso	Cantidad	Costo	Total
Opcional	Computador portátil	2	S/ 1,800.00	S/ 3,600.00
Opcional	Computador de escritorio	1	S/ 2,000.00	S/ 2,000.00
Licencias				**S/ 2,355.00**
Necesidad	Recurso	Cantidad	Costo	Total
Requerido	PILAR Basic	1	S/ 1,873.00	S/ 1,873.00
Requerido	ISO 22301:2014	1	S/ 482.00	S/ 482.00
Estimaciones de costos				
Estimación mínima				S/ 8,355.00
Estimación máxima				S/ 23,755.00

6. Tabla 6. Matriz de costos (Creación propia)

12. Desarrollo de la metodología

12.1. Entregable 1: Plan de negocio de Desarrollo A1

Contenido

12.1.1. Empresa y Objetivos

12.1.1.1. Misión

Ser una empresa competente y con presencia en el rubro. Que brinde un servicio reconocido por sus clientes por su eficacia y dedicación, teniendo importancia para sus clientes a tal punto de ser recomendada a otras empresas.

12.1.1.2. Visión

Ser la empresa número uno en el rubro de desarrollo de software del país.

12.1.2. Mercado Objetivo

Empresas pequeñas o medianas de cualquier rubro que quieran crear o mejorar su sitio web para aumentar las ventas de sus productos o servicios.

12.1.3. Marco Legal

MARCO LEGAL	DESCRIPCIÓN
NTP ISO/IEC 27001:2014	La Norma Técnica Peruana del Sistema de Gestión de la Seguridad de la Información, tiene como objetivo establecer un modelo para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización.
NTP ISO/IEC 27002:2017	Dentro del Código de prácticas para controles de seguridad de la información, se dará énfasis en el control A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio. Dicho control reacciona ante las interrupciones de las operaciones del negocio y busca proteger los procesos críticos de este. o A.17.1 Continuidad de la seguridad de la información Planificación, implementación, verificación, revisión y evaluación de la continuidad de la seguridad de la información o A.17.2 Redundancia Asegurar la disponibilidad de los recursos de tratamiento de la información.
Artículo 4 del Decreto	En el artículo de este Decreto Supremo se define el número de trabajadores y el monto de ventas por año

Supremo N° 007-2008	para ser considerado una MYPE. Los límites de ventas pueden ser cambiados cada dos años por otro Decreto Supremo del MEF.
Decreto Legislativo N° 28015 - Ley de promoción y formalización de las micro y pequeñas empresas	El Decreto Legislativo tiene como propósito fomentar la competitividad, formalización y desarrollo de las MYPES para incrementar el empleo sostenible, productividad y rentabilidad
LEY N° 27268 - Ley general de la pequeña y microempresa	La presente ley tiene como objetivo establecer el marco legal para la promoción y el desarrollo de las pequeñas y microempresas, normando políticas de alcance general y la creación de instrumentos de promoción, formalización y para la consolidación de los ya existentes, dentro de una economía sólida de mercado.
Resolución ministerial N° 124-2020 - EF/15 - Reglamento Operativo del Fondo de Apoyo Empresarial a la MYPE	Decreto de Urgencia que dicta medidas complementarias destinadas al financiamiento de la micro y pequeña empresa y otras medidas para reducir el impacto del COVID-19 en la economía peruana
Decreto Legislativo N° 1086 - Régimen Laboral Especial	Este Decreto Legislativo es necesario para poder poner trabajadores en planilla

12.1.4. Oportunidades y Mercado

12.1.4.1. Propuesta de Valor

En los últimos años se han extendido las ventas de productos y servicios por Internet, al punto de que se ha vuelto imprescindible que cada empresa cuente con su propio sitio web. Por este motivo, brindamos servicios de creación y auditoria de sitios web

completos, buscando optimizar la velocidad del sitio y el SEO para atraer más clientes potenciales. Así mismo, los sitios web creados pasan por un arduo proceso en la elección de los diseños y colores que tendrán, la organización o estructura de la página web y sus funciones dándole libertad completa al cliente para personalizar el sitio web a su antojo.

12.1.4.2. Segmento de Clientes

Empresas u organizaciones quienes busquen aumentar sus ventas por medio de Internet, creando un sitio web el cual exponga sus servicios o productos, o mejorando su sitio web ya existente.

12.1.4.3. Canales

Para la hacer efectiva la compra de algún servicio, previamente debe ponerse en contacto con la organización por medio de un correo electrónico o por nuestras redes sociales.

12.1.4.4. Relación con los Clientes

Las coordinaciones de los proyectos serán por medio de reuniones presenciales las cuales serán utilizadas para exponer ideas, presentación de avances y asesorías. También, se mandarán avances y se realizaran las coordinaciones las reuniones presenciales por correo electrónico.

12.1.4.5. Fuentes de Ingresos

Para la adquisición de la prestación de servicios se permite depósitos y pagos en efectivo.

12.1.4.6. Recursos Claves

- Equipos de oficina y el servidor de prueba.
- Proveedor de electricidad, proveedor de agua y proveedor de Internet.
- Personal calificado.

12.1.4.7. Actividades Claves

Creación y auditoria de sitios web.

12.1.4.8. Socios Claves

Empresas de desarrollo de software y empresas de marketing digital.

12.1.4.9. Estructura de Costos

Sueldos de los trabajadores, pago de servicios como electricidad, agua e internet, costes de infraestructura, costes por mantenimiento de equipos, página web, costes por publicidad.

12.1.5. Equipo y Activos

12.1.5.1. Organigrama

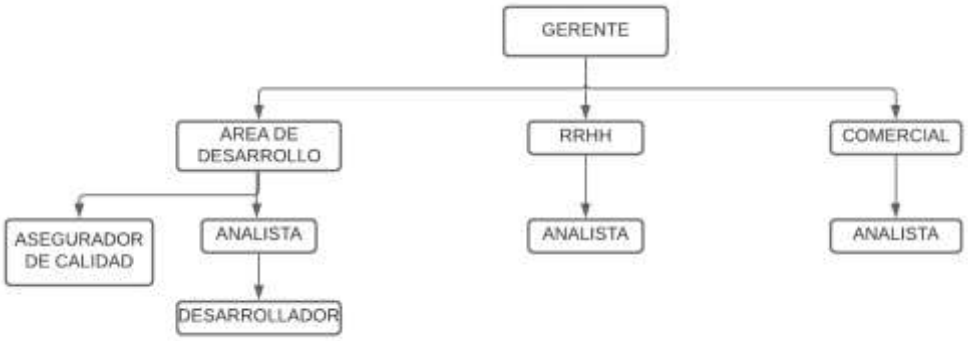
La empresa actualmente se encuentra constituida por 6 personas, las cuales cumplen distintos roles.

El gerente general es responsable de liderar la empresa, se encarga de la planificación de actividades, organizar los recursos, definir los objetivos y el rumbo de la empresa.

El área de desarrollo está constituida por tres personas, dos desarrolladores de software y una persona que cubre el rol de analista y asegurador de calidad del sitio web. Los desarrolladores se encargan de los procesos de en maquetación, diseño, programación y remediación, mientras que el analista se encarga de los procesos de planificación, auditoria y seguimiento del proyecto.

En el área de recursos humanos se encuentra una persona que cumple el rol de analista de recursos humanos, esta persona se encarga de mantener en regla la documentación de los trabajadores, pago de planillas, contratación de personal y mantenimiento del plantel laboral.

En el área comercial se encuentra una persona que cumple el rol de analista comercial, esta persona se encarga de atraer y mantener clientes con el fin de obtener ventas.



12.1.5.2. Lista de Activos

Inventario		
Responsable	**Características**	**Precio**
Analista - Personal	(2)Laptop HP Pavilion Procesador: Ryzen 5 3500U RAM: 12GB Almacenamiento: 512GB SSD	S/ 5,598.00
Analista - Servidor	Procesador: 4 núcleos RAM: 7GB Almacenamiento: 1000 GB disco duro *****https://azure.microsoft.com/es-es/pricing/details/cloud-services/*****	$ 233.60/mes
Desarrollador 1	(2)Laptop HP Pavilion Procesador: Ryzen 5 3500U RAM: 12GB Almacenamiento: 512GB SSD	S/ 5,598.00

Desarrollador 2	(2)Laptop HP Pavilion Procesador: Ryzen 5 3500U RAM: 12GB Almacenamiento: 512GB SSD	S/ 5,598.00
RRHH	Laptop Lenovo Procesador: Ryzen 3 RAM: 4GB Almacenamiento: 128GB SSD	S/ 1,400.00
Comercial	Laptop Lenovo Procesador: Ryzen 3 RAM: 4GB Almacenamiento: 128GB SSD	S/ 1,400.00
Gerente	Laptop HP Pavilion Procesador: Core i5 RAM: 8GB Almacenamiento: 1TB	S/ 2,400.00

12.1.6. Servicios

12.1.6.1. Desarrollo de Sitios Web

Desarrollo de aplicaciones web personalizadas para cubrir las necesidades de la empresa.

- **Explicación**

El proceso de creación de un sitio web óptimo para las necesidades solicitadas consta de 6 procesos, los cuales aseguran la calidad y eficiencia del sitio web que será creado.

a. Recopilación de información: Esta es la tarea más importante ya que dará un contexto claro de los objetivos de la organización con el fin entender el público objetivo que la empresa desea atraer y sus objetivos principales.

   Se realizará un plan detallado sobre de las tecnologías que se utilizarán, la estrategia SEO para atraer potenciales clientes, la organización de la información, etc.

b. Planificación: En esta tarea se crea un wireframe, en el cual se debe mostrar un bosquejo del funcionamiento del sitio web y así medir que tan sencillo será para el usuario final encontrar la información o el servicio que requiera adquirir.

c. Diseño del sitio web: En esta tarea se le da forma al sitio web, se definen los colores, logotipos, tipos de letra, etc. La información recopilada en la primera tarea será de suma importancia para la elección de los estilos del sitio web. Por otro lado, esta tarea se repetirá hasta que el cliente se encuentre completamente satisfecho.

d. Creación de contenido: En esta tarea se realiza una recopilación de la información que se desea mostrar para ser agregada al sitio web. Las entradas creadas tendrán como fin llamar a alguna acción, la cual puede ser adquirir un servicio o producto o seguir navegando por el sitio web.

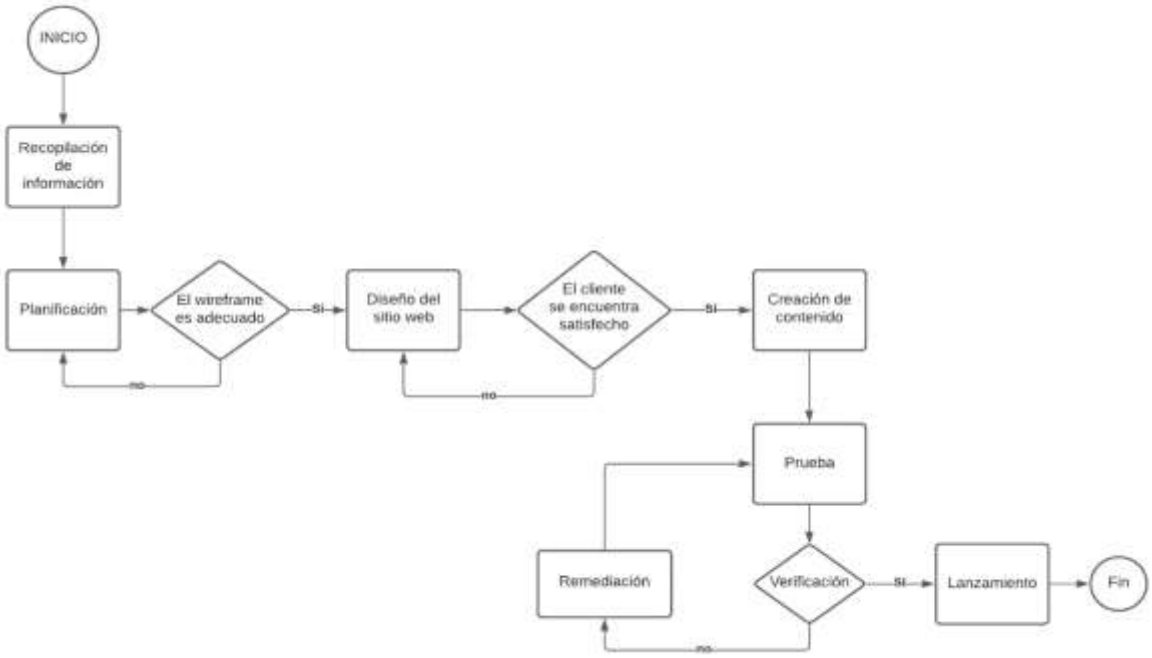
   El cliente tendrá que proporcionar el contenido del sitio web. Así mismo, antes de pasar a la siguiente tarea es necesario verificar que toda la información recopilada se encuentre en entradas.

e. Prueba: Esta tarea se realiza al terminar el sitio web, antes de pasar a la fase de producción. Se verifica el sitio web, se carga el sitio web en el hosting y se configura el dominio. Se realizan pruebas en búsqueda de posibles vulnerabilidades, pruebas de estrés de ancho de banda y auditoria de SEO para identificar posibles correcciones.

f. Remediación: En caso de encontrar algún fallo, se procederá a su remediación y volverá a realizarse la tarea “Prueba”.

g. Lanzamiento: Cuando la aplicación pasa todas las pruebas, se procede a lanzar la aplicación web en el servidor Cloud.

- **Flujograma**



12.1.6.2. Auditoria de Seguridad para Aplicaciones Web

Auditoria de seguridad que busca encontrar y reportar vulnerabilidades que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de una aplicación web.

- **Explicación**

a. Reconocimiento: Esta fase consiste en la recolección de información del objetivo, de esta manera mejorara la comprensión del sistema objetivo y se realizaran escaneos y pruebas más personalizadas.

   Dentro de esta fase se trata de obtener el hostname, IP, sistema operativo, puertos abiertos, servicios que se estén corriendo, versión de servicios, encontrar subdominios, etc.

b. Escaneo: En la fase de escaneo se busca encontrar información relevante sobre posibles vulnerabilidades que la aplicación web pueda tener y se valida la información recolectada en la fase previa.
   Los escaneos se realizan tanto manual como por medio de aplicaciones que facilitan esta labor como Nikto, Burpsuite, OWASP ZAP, SQLmap, etc.
c. Prueba: Se realizan pruebas sobre las posibles vulnerabilidades existentes en la aplicación web. Las pruebas se dividen en las siguientes categorías:
   - Prueba de configuración y despliegue
   - Pruebas de gestión de identificación
   - Pruebas de autenticación
   - Pruebas de autorización
   - Pruebas de gestión de sesiones
   - Pruebas de validación de entrada
   - Pruebas de manejo de errores
   - Pruebas de cifrado
   - Pruebas de lógica de negocio
   - Pruebas de lado del cliente
d. Reporte & Documentación: En esta última etapa, se presenta todas las vulnerabilidades que hayan sido encontradas dentro de las pruebas con detalles de cómo se encontró, severidad, impacto y solución.
   - **Flujograma**

12.2. Entregable 2: Acta de constitución del Sistema de Gestión de Continuidad del Negocio

CONTENIDO

12.2.1. Información del proyecto

Datos

Empresa / Organización	Auditores Externos
Proyecto	Diseño de un Sistema de Gestión de Continuidad del Negocio
Fecha de preparación	18/09/2020
Cliente	Desarrollo A1
Gerente de proyecto	Gerente general de Desarrollo A1

Patrocinador / Patrocinadores

Nombre	Cargo
Pedro Vargas	**Auditor**
Sebastian Velazquez	**Auditor**

12.2.2. Propósito y justificación del proyecto

Proporcionar a la empresa auditada el Diseño de un Sistema de Gestión de Continuidad del Negocio aplicable a su contexto.

12.2.3. Descripción del proyecto y entregables

Este proyecto tiene como entregables

- Actas de reuniones
- Matriz BIA
- Análisis de riesgos
- Planes de continuidad

12.2.4. Requerimientos de alto nivel

Requerimientos del proyecto

Documentos de la empresa
Matriz RACI
Servicios y productos

12.2.5. Objetivos

Objetivo	Indicador de éxito
Alcance	
Análisis de riesgo basado en la información proporcionada	Entrega del BIA y análisis de riesgos
Formulación de planes y estrategias de continuidad	Entrega de planes

Objetivo	Indicador de éxito
Entrega de documentación estipulada en el los entregables del proyecto	Entrega de documentación propuesta.
Limitantes	
No se realiza la implementación del SGCN	
Cronograma (Tiempo)	
Etapa 1 (07/09/2020 – 01/10/2020)	Cumplir con los entregables
Etapa 2 (02/10/2020 – 11/11/2020)	Cumplir con los entregables
Etapa 3 (12/11/2020 – 23/11/2020)	Cumplir con los entregables
Costo	
Reducción de costos con personal actual en planilla	
Reducción de costos con equipos del personal actual	
Presupuesto aceptable para pequeñas empresas	
Calidad	
Sistema de gestión aplicable a pequeñas empresas	

12.2.6. Premisas y restricciones

Todos los roles de los planes de continuidad deben ser asumidos por el personal actual de la empresa para poder cumplir con los objetivos del proyecto

12.2.7. Riesgos iniciales de alto nivel

- Documentación necesaria incompleta
- Personal insuficiente para asignación de responsabilidades
- Falta de conocimiento de servicios y activos críticos

12.2.8. Cronograma de hitos principales

Hito	Fecha tope
Reunión inicial y entrega de acta de constitución	**18/09/2020**
Análisis de Impacto al Negocio	**21/10/2020**
Análisis de Riesgos	**21/10/2020**
Entrega de planes de continuidad	**11/11/2020**
Reunión final	**23/11/2020**

12.2.9. Presupuesto inicial asignado

S/. 8355.00

12.2.10. Requisitos de aprobación del proyecto

- Diseño del Sistema de Gestión de continuidad del Negocio
- Cumplimiento de todos los entregables comprometidos
- Cumplimiento fecha inicio y fin del proyecto
- Presupuesto final no exceda S/. 9000.00

12.2.11. Criterios de cierre o cancelación

- El personal actual no puede cumplir con los roles que se le asignarán.
- No contar con el equipamiento necesario y la compra exceda el presupuesto límite.

12.2.12. Asignación del gerente de proyecto y nivel de autoridad

Gerente de proyecto

Nombre	Cargo
-	Gerente general de Desarrollo A1

Niveles de autoridad

Área de autoridad	Autoridad
Decisiones de personal (Staffing)	**Gerente general**
Gestión de presupuesto y de sus variaciones	**Gerente general**
Decisiones técnicas	**Desarrollador**
Resolución de conflictos	**Analista de calidad**
Facilitador de escalamiento	**Todos**
Limitador de autoridad	**Gerente general**

Personal y recursos preasignados

Recurso	Departamento / División
Gerente de proyecto	Gerente General

Recurso	Departamento / División
Implementador de SGCN	Auditor Externo
Supervisor Operacional de Continuidad	Analista de calidad
Miembro de equipo de desarrollo	Desarrollador
Miembro de equipo de desarrollo	Desarrollador

12.2.13. Aprobaciones

Patrocinador	Firma
Gerente General Desarrollo A1	
Auditor Externo	
Responsable técnico	
Supervisor operacional	

12.3. Entregable 3: Acta de reunión y listado de riesgos potenciales

LUGAR DE REUNIÓN: Zoom Meeting	HORA DE INICIO: 9:00 AM
FECHA: 16 de Noviembre 2020	HORA DE TERMINACIÓN: 3:00 PM
ELABORADO POR: Consultores SGCN	NUMERO DE ACTA: 002

12.3.1. Objetivos de la reunión

1. Comprender los riesgos latentes dentro de la empresa Desarrollo A1, para posteriormente ser analizados.

12.3.2. Agenda propuesta

1. Presentación del proyecto al equipo de Desarrollo A1
2. Se realizarán grupos entre los integrantes del equipo de Desarrollo A1 para exponer sus ideas.
3. Cierre.

12.3.3. Lista de Riesgos Clasificados

1. Desastres naturales
   - Huaicos
   - Sismos
   - Deslizamientos de terreno
   - Calor
2. Problemas externos o de proveedores
   - Fallas con el servicio eléctrico
   - Fallas con el servicio de Internet
   - Fallas con el servicio de agua potable
3. Problemas internos o averías en los servicios básicos
   - Fallas con el servicio eléctrico
   - Fallas con el servicio de Internet
   - Fallas con el servicio de agua potable
4. Averías de hardware
   - Fallas de componentes del servidor
   - Fallas de componentes en laptops de los colaboradores
   - Degradación de los soportes de almacenamiento
5. Problemas de software
   - Incompatibilidad de software con sistema operativo
   - Incompatibilidad de software con otro software
   - Falta de soporte
6. Errores y fallos no intencionados
   - Errores de colaboradores
   - Errores de monitorización
   - Errores de configuración
   - Difusión de software dañino
   - Fuga de información

- Alteración de información
- Destrucción de información
- Vulnerabilidades de los programas
- Errores de mantenimiento de programas
- Errores de parchado de software
- Errores de mantenimiento preventivo o reactivo de equipos de colaboradores
- Errores de actualización de equipos de colaboradores
- Caída de sistemas por agotamiento de recursos
- Pérdida de equipos
- Indisponibilidad de personas por enfermedad
- Indisponibilidad de personas por cualidades

7. Posibles amenazas externas
   - Manipulación de los registros de actividades
   - Manipulación de los ficheros de configuración
   - Suplantación de identidad
   - Abuso de privilegios
   - Acceso no autorizado
   - Análisis del tráfico
   - Interceptación de información
   - Difusión de malware
   - Destrucción de información
   - Modificación de información
   - Manipulación de software y hardware
   - Ataques de denegación de servicios
   - Robo de equipos
   - Extorsión
   - Ataques de ingeniería social
8. Problemas en los servicios brindados o con los clientes

- Falta de adaptación a los cambios
- No contar con personal calificado para trabajar sobre nuevas tecnologías
- El cliente realiza cambios imprevistos
- El cliente cancela un servicio
- Fallos al calcular el tiempo de un servicio

12.3.4. Participantes

- Gerente General
- Desarrollador 1
- Desarrollador 2
- Analista de calidad
- Analista comercial
- Analista de RRHH
- Consultores del SGCN

12.4. Entregable 4: Matriz RACI

Leyenda Matriz RACI	
Responsable	R
Aprobador	A
Consultado	C
Informado	I

	Desarrollador 1	**Desarrollador 2**	**Analista de calidad**	**Analista de RRHH**	**Analista comercial**	**Gerente general**
Recopilación de información	I	I	I	I	R	A
Planificación	C	C	I	I	R	A
Diseño	R	A	I	I	I	I
Implementación	R	A	I	I	I	I
Pruebas	C	C	R	I	I	I
Remediación	R	A	C	I	I	I
Puesta en producción	A	A	A	I	C	R


U T P
Universidad
Tecnológica
del Perú

12.5. Entregable 5: Listado de recursos asignados y Cronograma de concientización

12.5.1. Listado de Recursos asignados:

Inventario		
Responsable	**Características**	**Precio**
Analista - Personal	(2)Laptop HP Pavilion Procesador: Ryzen 5 3500U RAM: 12GB Almacenamiento: 512GB SSD	S/ 2,799.00
Analista - Servidor	Procesador: 4 núcleos RAM: 7GB Almacenamiento: 1000 GB disco duro *****https://azure.microsoft.com/es-es/pricing/details/cloud-services/*****	$ 233.60/mes
Desarrollador 1	(2)Laptop HP Pavilion Procesador: Ryzen 5 3500U RAM: 12GB Almacenamiento: 512GB SSD	S/ 2,799.00
Desarrollador 2	(2)Laptop HP Pavilion Procesador: Ryzen 5 3500U RAM: 12GB Almacenamiento: 512GB SSD	S/ 2,799.00
RRHH	Laptop Lenovo Procesador: Ryzen 3 RAM: 4GB Almacenamiento: 128GB SSD	S/ 1,400.00
Comercial	Laptop Lenovo Procesador: Ryzen 3 RAM: 4GB	S/ 1,400.00

	Almacenamiento: 128GB SSD	
Gerente	Laptop HP Pavilion Procesador: Core i5 RAM: 8GB Almacenamiento: 1TB	S/ 2,400.00

12.5.2. Cronograma de Sensibilización:

Actividades a Desarrollar	Fecha
Concientización sobre Riesgos Informáticos	24/09/2020
Concientización sobre Continuidad de Negocio	25/09/2020

LUGAR DE REUNIÓN: Zoom Meeting
FECHA: 24 de Septiembre 2020
ELABORADO POR: Consultores SGCN

HORA DE INICIO: 9:00 AM
HORA DE TERMINACIÓN: 1:00 PM
NUMERO DE ACTA: 003

OBJETIVOS DE LA REUNIÓN	
1.	Capacitar a los trabajadores para que entiendan la importancia de proteger correctamente la información de la organización
2.	Explicar métodos comunes de ataques realizados por cibercriminales

AGENDA PROPUESTA

1.	Introducción sobre seguridad de la información
2.	Protección de datos digitales
3.	Protección de identidad
4.	Ataques comunes de Ingeniería Social
5.	Seguridad en Redes Sociales
6.	Seguridad en Dispositivos Móviles
7.	Impacto sobre el negocio
8.	Cierre.

Conclusiones
Los trabajadores reconocen e identificar las amenazas existentes en el ciberespacio. Los trabajadores aplican estrategias para la protección de sus datos personales y los datos de la empresa. Los trabajadores entienden el impacto que puede tener que un cibercriminal obtenga información confidencial de la empresa.

PARTICIPANTES
Gerente General
Desarrollador 1
Desarrollador 2
Analista de calidad
Analista comercial
Analista de RRHH
Consultores del SGCN

LUGAR DE REUNIÓN: Zoom Meeting	HORA DE INICIO: 9:00 AM
FECHA: 25 de Septiembre 2020	HORA DE TERMINACIÓN: 1:00 PM

ELABORADO POR: Consultores SGCN	NUMERO DE ACTA: 004

OBJETIVOS DE LA REUNIÓN	
1.	Capacitar a los trabajadores para que entiendan el impacto negativo que puede tener el cese de operaciones en una empresa.

AGENDA PROPUESTA	
1.	Introducción sobre continuidad de negocio
2.	¿Por qué es importante la continuidad de negocio?
3.	Amenazas comunes (naturales, hombre, tecnología)
4.	Casos de éxito de empresas que aplicaron correctamente la continuidad de negocio
8.	Cierre.

Conclusiones
Los trabajadores entienden el impacto que puede tener el cese de las operaciones en la organización. Los trabajadores reconocen la importancia de contar con un SGCN y todo lo que este aporta a la empresa.

PARTICIPANTES
Gerente General
Desarrollador 1
Desarrollador 2
Analista de calidad
Analista comercial
Analista de RRHH
Consultores del SGCN

12.6. Entregable 6: Análisis de Impacto al Negocio

12.6.1. Criterios de evaluación de impactos

Impacto (Peso %)	Muy bajo (1)	Bajo (2)	Medio (3)	Alto (4)	Muy Alto (5)
Económico (38%)	La interrupción del proceso no genera pérdidas financieras	La interrupción del proceso genera pérdidas financieras mínimas para la empresa	La indisponibilidad del proceso genera pérdidas menores para el negocio dentro del límite aceptable para la empresa	La indisponibilidad del proceso genera pérdidas financieras considerables para la organización.	La indisponibilidad del proceso genera pérdidas financieras inaceptables que el negocio no tiene previsto dentro del presupuesto.
Operacional (32%)	La interrupción del proceso es imperceptible	La interrupción del proceso no dificulta las operaciones entre la empresa y el cliente	La indisponibilidad del proceso genera retrasos dentro del límite de tiempo aceptable de recuperación	La indisponibilidad del proceso genera el cese parcial de la operatividad del negocio, superando el	La indisponibilidad del proceso genera el cese total de la operatividad imposibilitando la recuperación

				límite de tiempo aceptable de recuperación	
Desarrollo de Marca (20%)	La interrupción del proceso no genera comentarios negativos para el negocio	La interrupción del proceso genera comentarios de inconformidad por clientes	La indisponibilidad del proceso genera comentarios negativos de los clientes y otras empresas	La indisponibilidad del proceso genera comentarios que afectan la reputación del negocio frente a clientes y potenciales clientes	La indisponibilidad del proceso genera pérdida de clientes e incredibilidad en el rubro
Legal (10%)	La interrupción del proceso no genera multas ni sanciones	La interrupción del proceso genera multas y sanciones mínimas para el negocio.	La indisponibilidad del proceso genera multas o perdidas de contratos aceptables	La indisponibilidad del proceso genera multas o pérdidas de contrato los cuales afectan a	La indisponibilidad del proceso genera perdida de contratos o incumplimiento legales

				la organización, provocando intervención regulatoria formal.	ocasionando multas o sanciones legales
	<= 15%	<= 25%	<= 50%	<= 75%	<= 100%

12.6.2. Matriz de procesos críticos

Identificación de Procesos Críticos												
Proceso	**Sub Proceso**	**Responsable**	**Económico (38%)**		**Operacional (32%)**		**Desarrollo de Marca (20%)**		**Legal (10 %)**		**Resultados**	**¿Proceso Crítico?**
Desarrollo de Sitios Web	Recopilación de información	Analista comercial	1	0.38	3	0.96	2	0.4	1	0.1	1.8	NO
	Planificación del servicio	Analista comercial	1	0.38	3	0.96	2	0.4	1	0.1	1.8	NO

	Diseño del sitio web	Desarrollador	4	1.52	4	1.28	2	0.4	3	0.3	3.5	SI
	Creación de contenido del sitio web	Desarrollador	4	1.52	3	0.96	1	0.2	3	0.3	3.0	NO
	Pruebas del sitio web	Analista de calidad	4	1.52	4	1.28	2	0.4	2	0.2	3.4	NO
	Remediación	Desarrollador	4	1.52	4	1.28	2	0.4	1	0.1	3.3	NO
	Puesta en producción	Gerente	4	1.52	3	0.96	4	0.8	5	0.5	3.8	SI
Auditoria de Seguridad para Aplicaciones Web	Recopilación de información	Analista de calidad	1	0.38	1	0.32	1	0.2	2	0.2	1.1	NO
	Escaneo de vulnerabilidades	Analista de calidad	1	0.38	3	0.96	2	0.4	2	0.2	1.9	NO
	Pruebas de explotación	Analista de calidad	4	1.52	4	1.28	3	0.6	2	0.2	3.6	SI

	Elaboración de informe final	Analista de calidad	2	0.76	3	0.96	2	0.4	2	0.2	2.3	NO
	Aprobación y envío de informe final	Gerente	4	1.52	2	0.64	4	0.8	5	0.5	3.5	SI

12.7. Entregable 7: Análisis de Riesgos

IDENTIFICACIÓN DE PELIGRO				
ÁREA	**ACTIVIDAD**	**CAUSA**	**RIESGO**	**CONSECUENCIA**
Es físicamente donde se realiza la actividad	La actividad que se lleva a cabo, de la cual surgen los riesgos	Motivo o razón para obrar de una manera determinada	Explicar la situación que causa la aparición de un peligro	Son las posibles consecuencias en caso se materialice el riesgo

MAGNITUD DE PROBABILIDAD		
1	Muy Bajo	1 o ninguna vez en un mes
2	Bajo	2 veces en un mes
3	Medio	3 a 4 veces en un mes
4	Alto	5 a 6 veces en un mes
5	Crítico	7 a más en un mes

MAGNITUD DE IMPACTO NEGATIVO		
VALOR	IMPACTO	DESCRIPCIÓN
1	Muy Bajo	Retrasa el proceso menos de una hora
2	Bajo	Retrasa el proceso de 2 a 6 horas
3	Medio	Retrasa el proceso de 7 a 20 horas
4	Alto	Retrasa el proceso de 21 a 42 horas
5	Crítico	Retrasa el proceso más de 43 horas

PROBABILIDAD X IMPACTO	Muy Bajo	Bajo	Medio	Alto	Crítico
Muy Bajo	1	2	3	4	5
Bajo	2	4	6	8	10
Medio	3	6	9	12	15
Alto	4	8	12	16	20
Crítico	5	10	15	20	25

1 2	3 4	5 6 7 8 9 10	11 12 13 14 15 16 17 18 19	20 21 22 23 24 25
MUY BAJO	BAJO	MEDIO	ALTO	CRÍTICO

	Muy Baja	Baja	Media	Alta	Crítica
Evitar					X
Mitigar			X	X	
Transferir				X	
Explotar					X
Mejorar			X	X	

Compartir			X
Aceptar	X	X	

IDENTIFICACIÓN DE PELIGRO						EVALUACIÓN DE RIESGOS		
ID	**RESPONSABLE**	**SUBPROCESO**	**CAUSA**	**RIESGO**	**CONSECUENCIA**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
1	Desarrollador	Diseño del sitio web	Movimientos sísmicos en el país debido a que se encuentra en una ubicación geográfica sísmica	Sismos	Inhabilitación para continuar con las actividades	1	5	5
2	Desarrollador	Diseño del sitio web	Fallos de fábrica	Recursos tecnológicos insuficientes	El equipo tiene que ser llevado por la garantía	1	5	5

3	Desarrollador	Diseño del sitio web	Vida útil del componente	Recursos tecnológicos insuficientes	Pérdida de información	1	4	4
4	Desarrollador	Diseño del sitio web	Vida útil del componente	Recursos tecnológicos insuficientes	Cese momentáneo de las actividades programadas	1	2	2
5	Desarrollador	Diseño del sitio web	Fallas de componentes en laptops de los colaboradores	Recursos tecnológicos insuficientes	Pérdida de información	1	4	4
6	Desarrollador	Diseño del sitio web	Fallas de componentes en laptops de los colaboradores	Recursos tecnológicos insuficientes	Cese momentáneo de las actividades programadas	1	2	2
7	Desarrollador	Diseño del sitio web	Falta de conocimiento	Errores de configuración	Detener el diseño del sitio web y levantar	3	2	6

					las observaciones de los errores			
8	Desarrollador	Diseño del sitio web	Inexistencia de políticas recurrentes de actualización y parcheo de vulnerabilidades	Vulnerabilidades en los softwares	Detener el diseño del sitio web e invertir tiempo en actualizaciones	1	4	4
9	Desarrollador	Diseño del sitio web	Contagio por enfermedades comunes	Indisponibilidad de personas por enfermedad	Reducción de capacidad operativa	2	3	6
10	Desarrollador	Diseño del sitio web	Contagio por COVID-19	Indisponibilidad de personas por enfermedad	Reducción de capacidad operativa	1	5	5
11	Desarrollador	Diseño del sitio web	Conexión a sitios web	Infección por malware	Se infecta con malware los	3	4	12

			maliciosos		equipos y/o servidores			
12	Desarrollador	Diseño del sitio web	Descarga de recursos no oficiales	Infección por malware	Se infecta con malware los equipos y/o servidores	4	4	16
13	Desarrollador	Diseño del sitio web	Ataque por ransomware	Extorsión	Pérdida de información	1	5	5
14	Desarrollador	Diseño del sitio web	Ataques de ingeniería social	Divulgación de información	El cliente solicita cambios imprevistos	1	4	4
15	Desarrollador	Diseño del sitio web	Inconformidades con el desarrollo del producto	El cliente solicita cambios imprevistos	Restructuración del requerimiento y cambios en el diseño del sitio web	2	4	8
16	Desarrollador	Diseño del sitio web	Mala estimación en la creación del	Fallos al calcular el tiempo de un	Incumplimiento de acuerdos de contrato	1	4	4

			plan de proyectos	servicio				
17	Analista de calidad / Gerente	Puesta en producción	Movimientos sísmicos en el país debido a que se encuentra en una ubicación geográfica sísmica	Sismos	Inhabilitación para pasar a producción el sitio web	1	5	5
18	Analista de calidad / Gerente	Puesta en producción	Fallo de fabrica	Recursos tecnológicos insuficientes	El equipo tiene que ser llevado por la garantía	1	5	5
19	Analista de calidad / Gerente	Puesta en producción	Vida útil del componente		Pérdida de información	1	4	4
20	Analista de calidad / Gerente	Puesta en producción	Vida útil del componente	Recursos tecnológicos insuficientes	Cese momentáneo de las actividades	1	2	2

					programadas			
21	Analista de calidad / Gerente	Puesta en producción	Fallas de componentes en laptops de los colaboradores	Recursos tecnológicos insuficientes	Pérdida de información	1	4	4
22	Analista de calidad / Gerente	Puesta en producción	Fallas de componentes en laptops de los colaboradores	Recursos tecnológicos insuficientes	Cese momentáneo de las actividades programadas	1	2	2
23	Analista de calidad / Gerente	Puesta en producción	Errores de configuración	Indisponibilidad del sitio web públicamente	Volver a iniciar los subprocesos necesarios para realizar una correcta configuración	1	3	3

24	Analista de calidad / Gerente	Puesta en producción	Contagio por enfermedades comunes	Indisponibilidad de personas por enfermedad	Reducción de capacidad operativa	2	3	6
25	Analista de calidad / Gerente	Puesta en producción	Contagio por COVID-19	Indisponibilidad de personas por enfermedad	Reducción de capacidad operativa	1	5	5
26	Analista de calidad / Gerente	Puesta en producción	Realizar conexiones o consultas a sitios web maliciosos	Difusión de malware	Se infecta con malware los equipos y/o servidores	2	4	8
27	Analista de calidad / Gerente	Puesta en producción	Descarga de recursos no oficiales	Difusión de malware	Se infecta con malware los equipos y/o servidores	1	4	4
28	Analista de calidad / Gerente	Puesta en producción	Ataque por ransomware	Extorsión	Pérdida de información	1	5	5

29	Analista de calidad / Gerente	Puesta en producción	Ataques de ingeniería social	Divulgación de información	El cliente solicita cambios imprevistos	1	4	4
30	Analista de calidad / Gerente	Puesta en producción	Inconformidades con el producto final	El cliente realiza cambios imprevistos	Restructuración del requerimiento	3	4	12
31	Analista de calidad / Gerente	Puesta en producción	Mala estimación en la creación del plan de proyectos	Fallos al calcular el tiempo de un servicio	Incumplimiento de acuerdos de contrato	1	4	4
32	Analista de calidad	Pruebas de explotación	Movimientos sísmicos en el país debido a que se encuentra en una ubicación geográfica sísmica	Sismo	Inhabilitación para continuar con las pruebas	1	5	5

33	Analista de calidad	Pruebas de explotación	Fallo de fabrica	Recursos tecnológicos insuficientes	El equipo tiene que ser llevado por la garantía	1	5	5
34	Analista de calidad	Pruebas de explotación	Vida útil del componente	Recursos tecnológicos insuficientes	Pérdida de información	1	4	4
35	Analista de calidad	Pruebas de explotación	Vida útil del componente	Recursos tecnológicos insuficientes	Cese momentáneo de las actividades programadas	1	2	2
36	Analista de calidad	Pruebas de explotación	Fallas de componentes en laptops de los colaboradores	Recursos tecnológicos insuficientes	Pérdida de información	1	4	4
37	Analista de calidad	Pruebas de explotación	Fallas de componentes en laptops de los colaboradores	Recursos tecnológicos insuficientes	Cese momentáneo de las actividades programadas	1	2	2

38	Analista de calidad	Pruebas de explotación	El trabajador explota una vulnerabilidad que puede desencadenar una denegación de servicio	Generar un estado de denegación de servicio sobre el sitio web del cliente	Se imposibilita continuar con las pruebas hasta que el sitio web se restablezca	2	2	4
39	Analista de calidad	Pruebas de explotación	Robo de información al trabajador	Fuga de información	Detener las pruebas e informar las vulnerabilidades que hasta el momento se han encontrado	1	1	1
40	Analista de calidad	Pruebas de explotación	Vulnerabilidad 0 day	Vulnerabilidades en los softwares	Detener las pruebas e informar	1	1	1

41	Analista de calidad	Pruebas de explotación	Contagio por enfermedades comunes	Indisponibilidad de personas por enfermedad	Se detienen o ralentizan las pruebas	2	3	6
42	Analista de calidad	Pruebas de explotación	Contagio por COVID-19	Indisponibilidad de personas por enfermedad	Se detienen o ralentizan las pruebas	1	5	5
43	Analista de calidad	Pruebas de explotación	Subir archivos maliciosos al sitio web	Difusión de malware	Se infecta con malware los equipos y/o servidores	1	2	2
44	Analista de calidad	Pruebas de explotación	Fallos al calcular el tiempo de un servicio	Demora debido a la cantidad de pruebas a realizar sobre el dominio	No se culmina a tiempo con las pruebas	2	4	8

45	Analista de calidad	Pruebas de explotación	Problemas con el proveedor de servicios de hosting del cliente	Fallas de conectividad con el sitio web del cliente	Las pruebas toman más tiempo de lo debido	1	3	3
46	Analista de calidad	Pruebas de explotación	No se brindaron los permisos dentro de los dispositivos de seguridad del cliente	Bloqueo de comunicación con el sitio web	Imposibilita la realización de pruebas hasta que los permisos sean registrados en los dispositivos de seguridad del cliente	3	3	9

47	Analista de calidad	Pruebas de explotación	No se realizaron las coordinaciones previas	No permiten el acceso a las instalaciones de la organización por políticas de bioseguridad	No se puede iniciar con las pruebas de explotación	2	5	10
48	Analista de calidad	Pruebas de explotación	Se genera mucho tráfico al realizar las pruebas de explotación	Problemas de conexión con la VPN de la organización	No se puede continuar con las pruebas de explotación	4	3	12
49	Gerente	Aprobación y envío de informe final	Movimientos sísmicos en el país debido a que se encuentra en una ubicación geográfica	Sismo	Inhabilitación para continuar con las pruebas	1	5	5

			sísmica					
50	Gerente	Aprobación y envío de informe final	Fallo de fabrica	Recursos tecnológicos insuficientes	El equipo tiene que ser llevado por la garantía	1	5	5
51	Gerente	Aprobación y envío de informe final	Vida útil del componente	Recursos tecnológicos insuficientes	Pérdida de información	1	4	4
52	Gerente	Aprobación y envío de informe final	Vida útil del componente	Recursos tecnológicos insuficientes	Cese momentáneo de las actividades programadas	1	2	2
53	Gerente	Aprobación y envío de informe final	Fallas de componentes en laptops de los colaboradores	Recursos tecnológicos insuficientes	Pérdida de información	1	4	4

54	Gerente	Aprobación y envío de informe final	Fallas de componentes en laptops de los colaboradores	Recursos tecnológicos insuficientes	Cese momentáneo de las actividades programadas	1	2	2
55	Gerente	Aprobación y envío de informe final	Uso de listas blancas para correos electrónicos	El cliente no puede recibir el correo	Demora en la entrega del informe final	1	2	2
56	Gerente	Aprobación y envío de informe final	Contagio por enfermedades comunes	Indisponibilidad de personas por enfermedad	Demora en dar la aprobación del informe final	2	3	6
57	Gerente	Aprobación y envío de informe final	Contagio por COVID-19	Indisponibilidad de personas por enfermedad	Demora en dar la aprobación del informe final	1	5	5
58	Gerente	Aprobación y envío de informe final	Envío de un correo electrónico	No se puede enviar el reporte final al	Demora en la entrega del informe final	1	2	2

			incorrecto	cliente				
59	Gerente	Aprobación y envío de informe final	No conformidad con el servicio	El cliente realiza cambios imprevistos	Volver a iniciar los subprocesos necesarios para cumplir los nuevos requerimientos	2	4	8
60	Gerente	Aprobación y envío de informe final	Modificación de alcance	El cliente realiza cambios imprevistos	Volver a iniciar los subprocesos necesarios para cumplir los nuevos requerimientos	1	5	5
61	Gerente	Aprobación y envío de informe final	Mala estimación en la creación del plan de proyectos	Fallos al calcular el tiempo de un servicio	Incumplimiento de acuerdos de contrato	1	4	4

12.8. Entregable 8: Matriz de Medidas de Control y Medidas de Control Mejorada

ID	CAUSA	RIESGO	ESTRATEGIA DE RESPUESTA	MEDIDAS DE CONTROL
2	Fallo de fabrica	Recursos tecnológicos insuficientes	Mitigar	Tener una laptop extra por si algún trabajador presenta inconvenientes con su laptop
7	Falta de conocimiento	Errores de configuración	Mitigar	Efectuar un plan de supervisión y revisión de avances en actividades programadas

9	Contagio por enfermedades comunes	Indisponibilidad de personas por enfermedad	Mitigar	Capacitar a los desarrolladores para que en caso de que el analista enferme puedan avanzar con algunas pruebas de explotación
10	Contagio por COVID-19	Indisponibilidad de personas por enfermedad	Mitigar	Capacitar a los desarrolladores para que en caso de que el analista enferme puedan avanzar con algunas pruebas de explotación
11	Conexión a sitios web maliciosos	Infección por malware	Mitigar	Implementar sistema de seguridad para la detección y prevención de malware
12	Descarga de recursos no oficiales	Infección por malware	Mitigar	Implementar sistema de seguridad para la detección y prevención de malware
13	Ataque por ransomware	Extorsión	Mitigar	Implementar políticas de backup periódicos y sistemas de seguridad para detección de malware
18	Fallo de fabrica	Recursos tecnológicos insuficientes	Mitigar	Tener una laptop extra por si algún trabajador presenta inconvenientes con su laptop

24	Contagio por enfermedades comunes	Indisponibilidad de personas por enfermedad	Mitigar	Capacitar a los desarrolladores para que en caso de que el analista enferme puedan avanzar con algunas pruebas de explotación
25	Contagio por COVID-19	Indisponibilidad de personas por enfermedad	Mitigar	Capacitar a los desarrolladores para que en caso de que el analista enferme puedan avanzar con algunas pruebas de explotación
26	Conexión a sitios web maliciosos	Difusión de malware	Mitigar	Implementar sistema de seguridad para la detección y prevención de malware
28	Ataque por ransomware	Extorsión	Mitigar	Implementar políticas de backup periódicos y sistemas de seguridad para detección de malware
33	Fallo de fabrica	Recursos tecnológicos insuficientes	Mitigar	Tener una laptop extra por si algún trabajador presenta inconvenientes con su laptop
41	Contagio por enfermedades comunes	Indisponibilidad de personas por enfermedad	Mitigar	Capacitar a los desarrolladores para que en caso de que el analista enferme puedan avanzar con algunas pruebas de explotación

42	Contagio por COVID-19	Indisponibilidad de personas por enfermedad	Mitigar	Capacitar a los desarrolladores para que en caso de que el analista enferme puedan avanzar con algunas pruebas de explotación
44	Fallos al calcular el tiempo de un servicio	Demora debido a la cantidad de pruebas a realizar sobre el dominio	Mitigar	Analizar el alcance que tendrá el proyecto antes de iniciar el servicio
46	Problemas con soluciones de seguridad del cliente	Bloqueo de comunicación con el sitio web	Mitigar	Solicitar los permisos antes de iniciar las pruebas de explotación
47	No se realizaron las coordinaciones previas	No permiten el acceso a las instalaciones de la organización por políticas de bioseguridad	Mitigar	Realizar coordinaciones previas al día de las pruebas de explotación para seguir los protocolos de bioseguridad de la empresa cliente

48	Se genera mucho tráfico al realizar las pruebas de explotación	Problemas de conexión con la VPN de la organización	Mitigar	Iniciar las pruebas de explotación en las madrugadas, cuando el tráfico es menor
50	Fallo de fabrica	Recursos tecnológicos insuficientes	Mitigar	Tener una laptop extra por si algún trabajador presenta inconvenientes con su laptop
56	Contagio por enfermedades comunes	Indisponibilidad de personas por enfermedad	Mitigar	Poner a cargo al analista de calidad para la revisión el informe y su aprobación en caso el gerente general no se encuentre apto para dar su confirmación
57	Contagio por COVID-19	Indisponibilidad de personas por enfermedad	Mitigar	Poner a cargo al analista de calidad para la revisión el informe y su aprobación en caso el gerente general no se encuentre apto para dar su confirmación

ID	RIESGO SECUNDARIO (RS)	RIESGO RESIDUAL (RR)	NUEVA ESTRATEGIA DE RESPUESTA	MEDIDA DE CONTROL MEJORADA
2	-	Se necesitan programas e información que se encuentran en la laptop averiada	Mitigar	Utilizar copia de seguridad con sincronización automática de archivos importantes a la nube

7	El encargado de la supervisión no pueda asumir la carga operativa	-	Mitigar	Designar más de un responsable capacitado de asumir la responsabilidad
9	Los desarrolladores no tienen disponibilidad para realizar las pruebas de explotación	-	Transferir	Contratar a un tercero especialista en el tema para que pueda hacerse cargo del diseño del sitio web
10	Los desarrolladores no tienen disponibilidad para realizar las pruebas de explotación	-	Transferir	Contratar a un tercero especialista en el tema para que pueda hacerse cargo del diseño del sitio web
11	No contar con personal capacitado para administrar soluciones de seguridad	-	Transferir	Contratar a un tercero que se encargue de la administración o brinde asesoría al equipo de trabajo
12	No contar con personal capacitado para administrar soluciones de seguridad	-	Transferir	Contratar a un tercero que se encargue de la administración o brinde asesoría al equipo de trabajo

13	-	Menor pérdida de información	Aceptar	-
18	-	Se necesitan programas e información que se encuentran en la laptop averiada	Mitigar	Utilizar copia de seguridad con sincronización automática de archivos importantes a la nube
24	Los desarrolladores no tienen disponibilidad para realizar las pruebas de explotación	-	Transferir	Contratar a un tercero especialista en el tema para que pueda hacerse cargo de la puesta en producción del sitio web
25	Los desarrolladores no tienen disponibilidad para realizar las pruebas de explotación	-	Transferir	Contratar a un tercero especialista en el tema para que pueda hacerse cargo de la puesta en producción del sitio web
26	No contar con personal capacitado para administrar soluciones de seguridad	-	Transferir	Contratar a un tercero que se encargue de la administración o brinde asesoría al equipo de trabajo

28	-	Menor pérdida de información	Aceptar	-
33	-	Se necesitan programas e información que se encuentran en la laptop averiada	Mitigar	Utilizar copia de seguridad con sincronización automática de archivos importantes a la nube
41	Los desarrolladores no tienen disponibilidad para realizar las pruebas de explotación	-	Transferir	Contratar a un tercero especialista en el tema para que pueda hacerse cargo de las pruebas de explotación
42	Los desarrolladores no tienen disponibilidad para realizar las pruebas de explotación	-	Transferir	Contratar a un tercero especialista en el tema para que pueda hacerse cargo de las pruebas de explotación
44	Al momento de culminar el escaneo se encuentran varias páginas en el sitio web	-	Mitigar	Proponer un tiempo variable para la explotación de vulnerabilidades que dependa del alcance encontrado al momento del escaneo

46	-	No se brindaron correctamente los permisos	Mitigar	Al momento de brindar los accesos correspondientes, realizar pruebas de estrés para verificar no haya bloqueos de comunicaciones con el analista
47	-	Dentro de los protocolos del cliente, antes de ingresar a las instalaciones se solicita que el trabajador guarde aislamiento preventivo	Evitar	Solicitar brinden accesos por VPN
48	-	La conexión por VPN es inestable al realizar pruebas muy intrusivas o que generen mucho trafico	Mitigar	Solicitar que habiliten un equipo dentro de la red del cliente al cual se pueda acceder por medio de RDP para realizar las pruebas más intrusivas y que generan más tráfico desde dicho equipo

50	-	Se necesitan programas e información que se encuentran en la laptop averiada	Mitigar	Utilizar copia de seguridad con sincronización automática de archivos importantes a la nube
56	El analista de calidad se encuentra indisponible por enfermedad	-	Aceptar	-
57	El analista de calidad se encuentra indisponible por enfermedad	-	Aceptar	-

12.9. Entregable 9: Matriz de requerimiento de recursos

MATRIZ DE REQUERIMIENTO DE RECURSOS			
Recurso	**Responsable**	**Información del recurso**	**Financiado**
Riesgo	**Recursos tecnológicos insuficientes**		

Laptop	Desarrollador Analista de Calidad	Disponer de al menos tres equipos adicionales en caso alguno de los colaboradores se vea afectado	SI
Servidor	Analista de Calidad	Disponer de un servidor adicional en caso se vea afectado el que está en uso	NO
Riesgo	**Errores de configuración**		
Rutina de plan de supervisión	Analista de calidad	Disponer de un plan de revisión periódico de avances en el desarrollo del sitio web del proyecto	SI
Analista de calidad	Analista de RRHH	Disponer de un analista de calidad adicional para que cubra con el plan de revisión establecido	NO
Desarrollador	Analista de RRHH	Disponer de un desarrollador adicional contratado por proyecto que cubra una necesidad en particular	NO
Riesgo	**Indisponibilidad de personas por enfermedad**		
Analista de calidad	Analista de RRHH	Disponer de un analista de calidad adicional para que cubra con el plan de revisión establecido	NO

Desarrollador	Analista de RRHH	La carga operativa del desarrollador enfermo debe ser cubierta por el otro desarrollador y el analista de calidad	SI
Analista comercial/RRHH	Analista de RRHH	Disponer de un analista que pueda hacer tanto de comercial o de RRHH	NO
Riesgo		**Infección por malware**	
Ingeniero de Soporte	Analista de RRHH	Contratar a un ingeniero que haga de soporte para las soluciones de seguridad a implementar Capacitar a un desarrollador o analista de calidad para que cubra con el perfil	NO
Solución de seguridad perimetral	Soporte técnico	Disponer de un firewall que sea administrado por el soporte para la seguridad perimetral	NO
Solución de seguridad en estación de trabajo	Soporte técnico	Disponer de un antivirus en las estaciones de trabajo de los colaboradores que sea administrado por el soporte	NO
Riesgo		**Extorsión**	

Backup	Analista de Calidad	Disponer de backups periódicos para poder restablecer la información	SI
Servidor	Analista de Calidad	Disponer de un espacio en el servidor dedicado a guardar las copias de backup	SI
Ingeniero de Soporte	Analista de RRHH	Contratar a un ingeniero que haga de soporte para las soluciones de seguridad a implementar Capacitar a un desarrollador o analista de calidad para que cubra con el perfil	NO
Solución de seguridad perimetral	Soporte técnico	Disponer de un firewall que sea administrado por el soporte para la seguridad perimetral	NO
Solución de seguridad en estación de trabajo	Soporte técnico	Disponer de un antivirus en las estaciones de trabajo de los colaboradores que sea administrado por el soporte	NO
Riesgo		**Difusión de malware**	

Ingeniero de Soporte	Analista de RRHH	Contratar a un ingeniero que haga de soporte para las soluciones de seguridad a implementar Capacitar a un desarrollador o analista de calidad para que cubra con el perfil	NO
Solución de seguridad perimetral	Soporte técnico	Disponer de un firewall que sea administrado por el soporte para la seguridad perimetral	NO
Solución de seguridad en estación de trabajo	Soporte técnico	Disponer de un antivirus en las estaciones de trabajo de los colaboradores que sea administrado por el soporte	NO
Riesgo	**Demora debido a la cantidad de pruebas a realizar sobre el dominio**		
Analista de calidad	Analista de RRHH	Disponer de otro analista de calidad de acuerdo con la magnitud del proyecto Capacitar a un desarrollador para que cuente con el mismo perfil y apoyar al analista de calidad	NO
Riesgo	**Bloqueo de comunicación con el sitio web**		
-			

Riesgo	**No permiten el acceso a las instalaciones de la organización por políticas de bioseguridad**		
VPN	Analista de Calidad	Disponer de una solución VPN para contar con un medio alterno de acceso a los recursos físicos del cliente	NO
Riesgo	**Problemas de conexión con la VPN de la organización**		
VPN	Analista de Calidad	Disponer de una solución VPN alterna en caso falle la que está en uso	NO

MATRIZ DE REQUERIMIENTO DE RECURSOS	
Recurso	**Descripción**
Servidor	Debe contar como mínimo con los mismos recursos que el servidor en uso actual. Se puede considerar uno con mayores recursos
Analista de calidad	Debe cubrir el perfil actual del analista de calidad
Desarrollador	Debe cubrir el perfil actual del desarrollador
Analista de RRHH	Debe cubrir el perfil actual del analista de RRHH. Esta contratación está sujeta a la necesidad y carga operativa que pueda recaer en el momento.
Analista comercial	Debe cubrir el perfil actual del analista comercial. Esta contratación está sujeta a la necesidad y carga operativa que pueda recaer en el momento.
Ingeniero de Soporte	Debe contar con experiencia mínima de 2 años en la administración de la solución de seguridad que se desea obtener y debe estar certificado en la misma de preferencia.
Solución de seguridad perimetral	Disponer de un Firewall con características mínimas de: Rendimiento de firewall (HTTP/appmix): 500 Mbps Rendimiento de prevención de amenazas (HTTP/appmix): 250 Mbps

	Rendimiento de IPSec VPN: 500 Mbps *Procurar que todas las soluciones de seguridad sean de la misma marca
Solución de seguridad en estación de trabajo	*Procurar que la marca del Firewall disponga de un cliente que cumpla con función de endpoint. **No hay especificaciones mínimas y se debe considerar uno en cada estación de trabajo.
VPN	*Procurar que el Firewall tenga un módulo VPN para que sea activa. **No hay especificaciones mínimas y se debe considerar uno en cada estación de trabajo.

12.10. Entregable 10: Plan de Continuidad del Negocio

Versión: Primera

Revisión: 10/11/2020

Principal responsable		
Gerente General	gerentegeneral@desarrolloa1.com	Cel: 973628344
Firma 		Documento de Identidad: 10145672

Responsable de seguridad		
Desarrollador 1	desarrollador1@desarrolloa1.com	Cel: 915273482
Firma 		Documento de Identidad: 42054111

Responsable de tecnologías		
Desarrollador 2	desarrollador2@desarrolloa1.com	Cel: 901283746
Firma 		Documento de Identidad: 07178990

Responsable de recuperación		
Analista de calidad	analistacalidad@desarrolloa1.com	Cel: 999129165
Firma 		Documento de Identidad: 09871230

12.10.1. Documentación Histórica

Registro histórico de actualización

Número de revisión	Fecha de revisión	Resumen de cambios	Autor
001	10/11/2020	Primero versión del documento	Auditor externo

Lista de distribución autorizada

Nombre	Posición	Compañía
Gerente General	Gerente General	Desarrollo A1
Analista de RRHH	Analista de RRHH	Desarrollo A1
Analista comercial	Analista comercial	Desarrollo A1
Desarrollador 1	Desarrollador 1	Desarrollo A1
Desarrollador 2	Desarrollador 2	Desarrollo A1
Analista de calidad	Analista de calidad	Desarrollo A1
Auditor	Auditor	Externo


U T P
Universidad
Tecnológica
del Perú

12.10.2. Introducción

La introducción del plan establece el propósito, aplicabilidad, alcance y supuestos para la Planificación de Continuidad del Negocio.

El Plan de Continuidad del Negocio (BCP, por sus siglas en inglés) permite que las actividades críticas continúen sin interrupciones cuando surgen eventos inesperados. Esta planificación debe resultar en la reducción del riesgo y menos tiempo en las fases de contingencia y/o recuperación al recuperar las operaciones impactadas.

El objetivo de este plan es brindar orientación a la empresa Desarrollo A1 para la restauración de las actividades. Cuando corresponda, este Plan de Continuidad del Negocio debe activarse.

Este plan describe el marco y los procedimientos que se activarán en caso de que ocurra un desastre, para permitir la recuperación de las actividades de la empresa Desarrollo A1.

Las principales actividades que apoyaran en el cumplimiento del objetivo de este plan son las siguientes:

- Minimizar las interrupciones de las operaciones normales.
- Limitar el alcance de las interrupciones y los daños.
- Minimizar el impacto económico de la interrupción.
- Establecer con anticipación medios alternativos de operación.
- Capacitar al personal en procedimientos de emergencia.
- Proporcionar una rápida restauración del servicio

Este plan establece procedimientos para recuperar los servicios críticos luego de una interrupción. Para cumplir con los objetivos listados se debe considerar:

- Maximizar la efectividad de las operaciones a través de las siguientes fases:
    - Fase de notificación / activación para detectar y evaluar daños y activar el plan
    - Fase de recuperación para restaurar operaciones temporales y evaluar daños al sistema

- Fase de reconstitución para restaurar las capacidades de procesamiento del sistema a las operaciones normales.

- Identificar las actividades, recursos y procedimientos necesarios.
- Asignar responsabilidades al personal designado y proporcionar orientación para la recuperación de los servicios críticos.
- Asegurar la coordinación con el resto del personal que participará en las estrategias de Planificación de Continuidad del Negocio.

12.10.2.1. Alcance

El alcance de los procedimientos documentados en este Plan de Continuidad del Negocio está restringido a los Servicios críticos proporcionados por la empresa Desarrollo A1.

El alcance de los procedimientos cubre los siguientes servicios:

Servicio	Descripción
Desarrollo de Sitios Web	Desarrollo de aplicaciones web personalizadas para cubrir las necesidades de los clientes.
Auditoria de Seguridad para Aplicaciones Web	Auditoria de seguridad que busca encontrar y reportar vulnerabilidades que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de una aplicación web.

12.10.2.2. Actividades críticas del negocio

Se identifican las actividades críticas de los servicios del negocio trasmitidas del resultado del análisis de impacto al Negocio previamente ejecutado. En el cuadro se debe tener en cuenta el período de tiempo máximo que el Plan de Continuidad del Negocio tolerará hasta que estas actividades críticas se vean afectadas.

Actividad crítica	Tiempo máximo aceptable de interrupción (MAO)	Impacto de incumplimiento
Diseño del sitio web	20 horas	Retraso en actividades consecuentes
Puesta en producción	16 horas	Retraso en entrega del producto
Pruebas de explotación	20 horas	Retraso en actividades consecuentes
Aprobación y envío de informe final	8 horas	Retraso en cierre de contrato

12.10.2.3. Prerrequisitos

Para que la recuperación de los servicios críticos sea eficaz, se debe considerar que:

- Se debe realizar una copia de seguridad adecuada de los datos fuera del sitio. Esto incluirá los datos del sistema.
- Se informará tanto a colaboradores como a clientes el estado y acuerdos que comprometerá la activación del plan.
- Se distribuirá una lista de los principales contactos del personal, incluidos los números de casa y las direcciones.
- Está en vigor un acuerdo firmado actual de este plan.
- Sitio físico de respaldo

12.10.2.4. Sitio físico de respaldo

En caso de que ocurriera un desastre que inhabilitara las oficinas clave, Desarrollo A1 ha dispuesto instalaciones alternativas donde la administración y el personal clave reanudarían las funciones comerciales más críticas de la organización. Inserte los detalles y la ubicación geográfica del sitio de recuperación

12.10.2.5. Sitio alterno para la continuidad del negocio

- Dirección: El Sol de la Molina Etapa I, La Molina
- Lima, Perú
- Número para comunicación: 389-1100
- Correo para comunicación: sede_lamolina@desarrolloa1.com

12.10.3. Enfoque de gestión

12.10.3.1. Políticas

Este capítulo conforma la declaración de las políticas (lineamientos) sobre la cuales se basará la planificación de la continuidad del negocio de la organización.

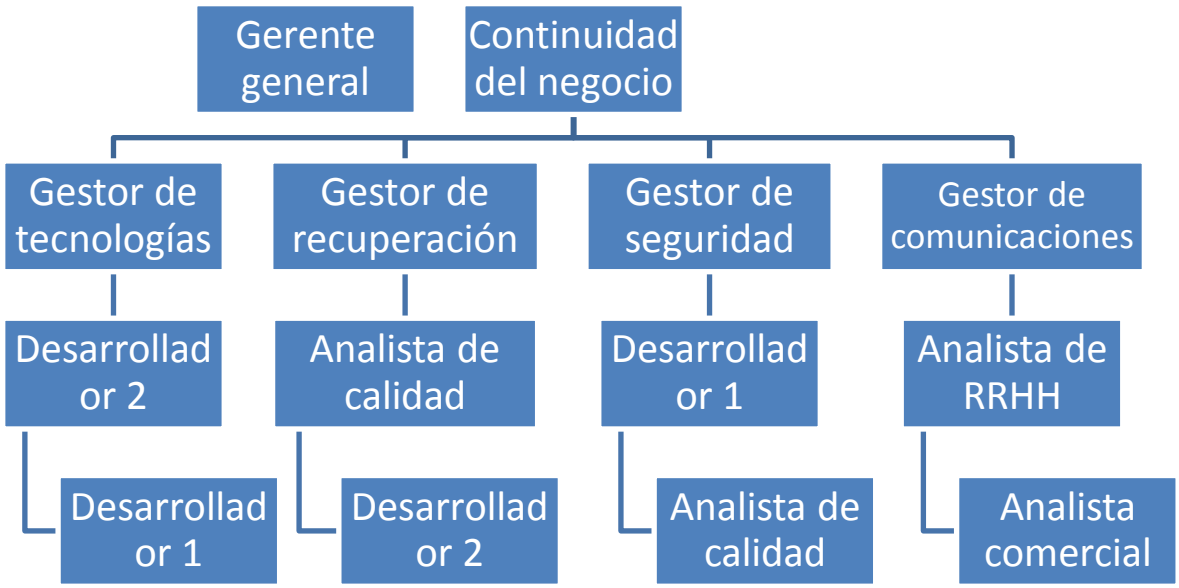
Este plan deberá cumplir con las siguientes políticas establecidas para el Plan de Continuidad del Negocio de la empresa Desarrollo A1:

- La organización debe desarrollar una capacidad de planificación y ejecución para que la interrupción no se extienda más allá de 42 horas.
- Los procedimientos para la ejecución de dicha capacidad se documentarán en un Plan de Continuidad del Negocio formal y se revisarán al menos una vez al año y se actualizarán según sea necesario.
- El personal responsable debe estar capacitado para ejecutar los procedimientos que les correspondan.
- El plan, las capacidades de recuperación y el personal deben realizar simulacros para identificar las debilidades de la capacidad al menos una vez al año.

12.10.3.2. Gobernanza

La empresa Desarrollo A1 debe establecer un orden de sucesión para garantizar que la autoridad para que la toma de decisiones del Plan de Continuidad del Negocio no se interrumpa.

EL siguiente organigrama define los miembros del equipo para la sucesión del responsable del plan.



12.10.3.3. Roles y Responsabilidades

Los miembros del equipo de la empresa Desarrollo A1 incluyen personal que es responsable de las operaciones diarias y el mantenimiento de los activos y servicios. La siguiente tabla

describe las responsabilidades de cada uno de los roles que conforma el equipo de trabajo de la empresa Desarrollo A1.

Rol	Teléfono celular	Correo	Responsabilidad
Gerente General	973628344	gerentegeneral@desarrolloa1.com	Principal responsable
Analista de RRHH	934657125	analistarrhh@desarrolloa1.com	Responsable de plan de comunicación
Analista comercial	994010014	analistacomercial@desarrolloa1.com	Responsable del mantenimiento
Desarrollador 1	915273482	desarrollador1@desarrolloa1.com	Responsable de seguridad
Desarrollador 2	901283746	desarrollador2@desarrolloa1.com	Responsable de tecnologías
Analista de calidad	999129165	analistacalidad@desarrolloa1.com	Responsable de plan de recuperación

12.10.4. Gestión de Riesgos

12.10.4.1. Disrupción deliberada

Examinar la situación potencial de desastre o emergencia causada por actividades que pueden describirse como "interrupción inducida". Las posibles interrupciones del negocio pueden ser causada por uno o más de los siguientes eventos:

Disrupción deliberada				
N °	Subproceso	Riesgo	Puntaje Riesgo	Nivel del Riesgo
1	Diseño del sitio web	Divulgación de información	4	Baja
2	Puesta en producción	Divulgación de información	4	Baja
3	Pruebas de explotación	Fuga de información	1	Baja

12.10.4.2. Desastres ambientales

Evaluar posibles desastres ambientales y situaciones de emergencia. Concéntrese en el nivel de interrupción del negocio que probablemente resulte de cada situación. Las posibles interrupciones del negocio pueden ser causada por uno o más de los siguientes eventos:

Desastres ambientales			
N °	Nombre	Puntaje Riesgo	Riesgo
1	Sismos	5	Media

12.10.4.3. Tecnología

Evaluar interrupciones causadas por medios tecnológicos. Las posibles interrupciones del negocio pueden ser causada por uno o más de los siguientes eventos:

Tecnología				
N °	Subproceso	Riesgo	Puntaje Riesgo	Nivel del Riesgo
1	Puesta en producción	Recursos tecnológicos insuficientes debido a que tiene que ser llevado a la garantía	5	Media
2	Pruebas de explotación	Recursos tecnológicos insuficientes debido a que tiene que ser llevado a la garantía	5	Media
3	Aprobación y envío de informe final	Recursos tecnológicos insuficientes debido a que tiene que ser llevado a la garantía	5	Media
4	Diseño del sitio web	Recursos tecnológicos insuficientes debido a que tiene que ser llevado a la garantía	5	Media
5	Puesta en producción	Recursos tecnológicos insuficientes por fallas en componentes de los colaboradores	4	Baja
6	Pruebas de explotación	Recursos tecnológicos insuficientes por fallas en componentes de los colaboradores	4	Baja

Tecnología				
7	Aprobación y envío de informe final	Recursos tecnológicos insuficientes por fallas en componentes de los colaboradores	4	Baja
8	Diseño del sitio web	Recursos tecnológicos insuficientes por fallas en componentes de los colaboradores	4	Baja
9	Pruebas de explotación	Problemas de conexión con la VPN de la organización	12	Alta
10	Aprobación y envío de informe final	Envío del correo electrónico del cliente incorrecto	2	Baja
11	Pruebas de explotación	Bloqueo de comunicación con el sitio web	9	Media
12	Pruebas de explotación	Ralentización del sitio web debido a ataques de DoS	8	Media
13	Diseño del sitio web	Errores de configuración	6	Baja
14	Pruebas de explotación	Generar un estado de denegación de servicio sobre el sitio web del cliente	4	Baja
15	Pruebas de explotación	Indisponibilidad del sitio web públicamente	3	Baja

Tecnología				
16	Aprobación y envío de informe final	El cliente no puede recibir el correo debido a que no se encuentra en la lista blanca	2	Baja
17	Pruebas de explotación	Fallas de conectividad con el sitio web del cliente	3	Baja

12.10.4.4. Seguridad Informática

Evaluar interrupciones causadas por vulneración de soluciones de seguridad. Las posibles interrupciones del negocio pueden ser causadas por uno o más de los siguientes eventos:

Seguridad Informática				
N °	Subproceso	Riesgo	Puntaje Riesgo	Nivel del Riesgo
1	Puesta en producción	Difusión de malware al descargar recursos no oficiales	4	Baja
2	Puesta en producción	Difusión de malware a través de realizar conexiones o consultas en sitios web maliciosos	8	Media
3	Pruebas de explotación	Realizar difusión de malware al subir archivos maliciosos al sitio web	2	Baja
4	Diseño del sitio web	Extorsión por infección de Ransomware	5	Media

Seguridad Informática				
5	Puesta en producción	Extorsión por infección de Ransomware	5	Media
6	Diseño del sitio web	Vulnerabilidades en los softwares	4	Baja
7	Pruebas de explotación	Vulnerabilidades en los software	4	Baja
8	Diseño del sitio web	Infección de malware por conexión a sitios web maliciosos	12	Alta
9	Diseño del sitio web	Infección de malware por descarga de recursos no oficiales	16	Alta

12.10.4.5. Otros posibles escenarios

Otros				
N °	Subproceso	Riesgo	Puntaje Riesgo	Nivel del Riesgo
1	Diseño del sitio web	Contagio por COVID-19	5	Media
2	Pruebas de producción	Contagio por COVID-19	5	Media
3	Pruebas de explotación	Contagio por COVID-19	5	Media
4	Aprobación y envío de informal final	Contagio por COVID-19	5	Media

Otros				
5	Diseño del sitio web	Contagio por enfermedades comunes	6	Media
6	Pruebas de producción	Contagio por enfermedades comunes	6	Media
7	Pruebas de explotación	Contagio por enfermedades comunes	6	Media
8	Aprobación y envío de informal final	Contagio por enfermedades comunes	6	Media
9	Pruebas de explotación	No permiten el acceso a las instalaciones de la organización por políticas de bioseguridad	10	Media
10	Aprobación y envío de informe final	El cliente realiza cambios imprevistos	12	Alta
11	Aprobación y envío de informe final	El cliente realiza cambios imprevistos	5	Media
12	Puesta en producción	El cliente realiza cambios imprevistos	8	Media
13	Diseño del sitio web	El cliente realiza cambios imprevistos	8	Media
14	Diseño del sitio web	Fallas al calcular el tiempo de un servicio	4	Baja
15	Puesta en producción	Fallas al calcular el tiempo de un servicio	4	Baja

Otros				
16	Aprobación y envío de informe final	Fallas al calcular el tiempo de un servicio	4	Baja

12.10.5. Estrategia de Continuidad

12.10.5.1. Estrategias de recuperación

La estrategia de restauración y recuperación describe los servicios relevantes para la recuperación. Este enfoque debe abarcar las necesidades y los pasos para reconstruir, modificar o reemplazar el hardware, sistema operativo o las aplicaciones, y de ser necesario, restaurar datos con el respaldo inmediato.

12.10.5.2. Tiempos de respuesta de recuperación

Se debe específica los tiempos de recuperación para cada uno de los servicios de la empresa.

N °	Servicio	Tiempo mínimo/promedio/máximo de recuperación	Observaciones
1	Desarrollo de Sitios Web	4/23/42 horas	El tiempo máximo de recuperación no puede superar el impacto de nivel Alto
2	Auditoria de Seguridad para Aplicaciones Web	2/22/42 horas	El tiempo máximo de recuperación no puede superar el impacto de nivel Alto

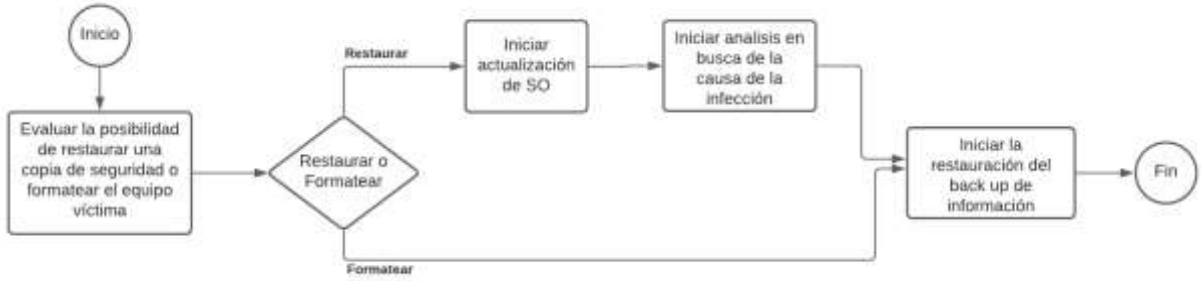
12.10.5.3. Procedimientos de recuperación

Se deben describir los métodos planificados para realizar la restauración de los servicios mencionados. Dada la magnitud del plan y el tamaño de la empresa objetivo, Desarrollo A1, la estrategia adecuada es la agrupación de los riesgos para poder ser abordados. A continuación, se detallan los grupos.

- Infección por Ransomware
- Problemas de Hardware
- Fallos de Conexión
- Conexiones maliciosas

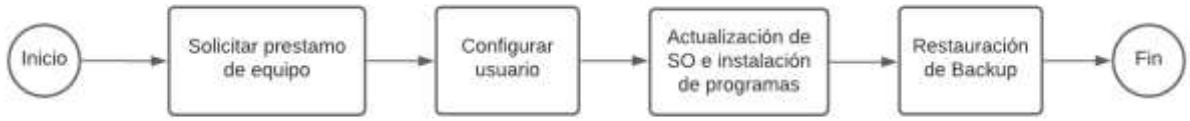
- Enfermedades
- Coordinación y planeación interna

Infección por Ransomware				
N °	Procedimiento de restauración	Responsable	Tiempo límite de ejecución	Aprobador
1	Evaluar la posibilidad de restaurar una copia de seguridad o si será necesario formatear el equipo víctima	Desarrollador 2	1 hora	Analista de calidad
2	En caso de realizar la restauración de la copia de seguridad, iniciar la actualización del sistema operativo	Desarrollador 2	2 horas	Analista de calidad
3	Iniciar un análisis en búsqueda del causante de la infección por malware	Desarrollador 1	4 horas	Analista de calidad
4	Realizar la restauración del back up almacenado en la solución Cloud	Desarrollador 2	2 horas	Analista de calidad



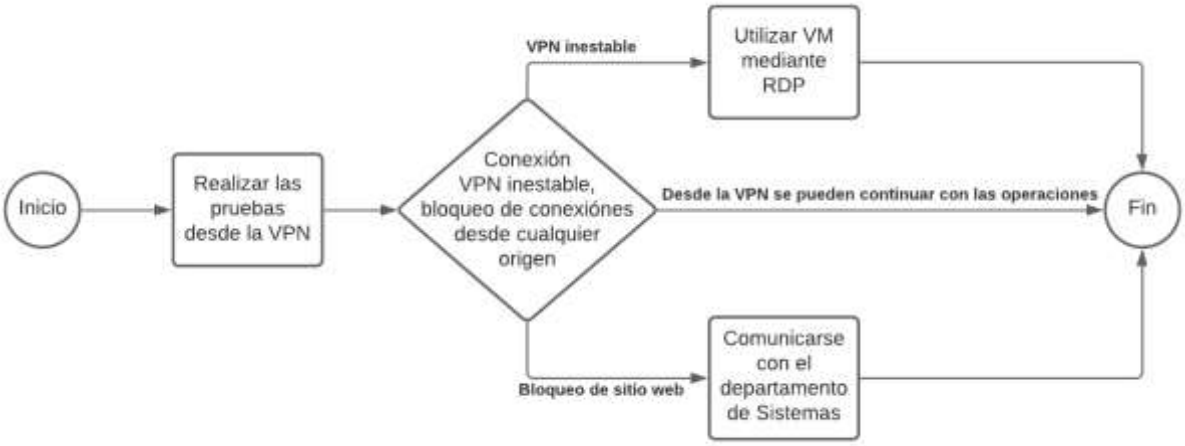
Flujograma 1. Procedimiento Infección por Ransomware

Problemas de Hardware				
N °	Procedimiento de restauración	Responsable	Tiempo límite de ejecución	Aprobador
1	Solicitar préstamo de equipo mientras la laptop del trabajador se encuentra en reparación	Analista de RRHH	1 hora	Gerente General
2	Configurar usuario del trabajador	Desarrollador 2	1 hora	Analista de calidad
3	Actualizar e instalar los programas necesarios para que el trabajador pueda cumplir con sus funciones principales	Desarrollador 2	1 hora	Analista de calidad
4	Realizar la restauración del back up almacenado en la solución Cloud	Desarrollador 2	2 horas	Analista de calidad



Flujograma 2. Procedimiento Problemas de Hardware

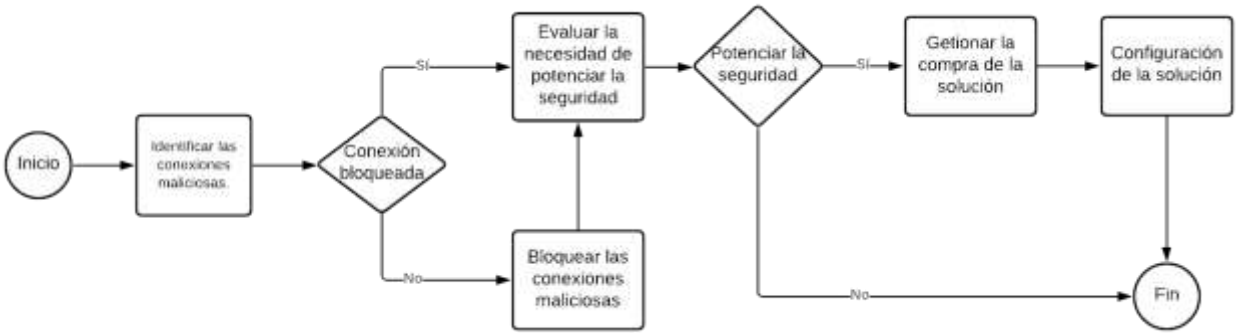
Fallos de Conexión				
N °	Procedimiento de restauración	Responsable	Tiempo límite de ejecución	Aprobador
1	Realizar las pruebas desde la red de la empresa por medio de la conexión VPN	Desarrollador 2	2 horas	Analista de calidad
2	En caso la conexión VPN sea inestable, realizar la conexión por RDP a la máquina virtual brindada por el cliente	Desarrollador 2	1 hora	Analista de calidad
3	En caso el sitio web haya bloqueado conexiones desde cualquier origen, comunicarse con el departamento de sistemas para que restablezcan el servidor web	Desarrollador 2	2 horas	Analista de calidad



Flujograma 3. Procedimiento Fallos de conexión

Conexiones maliciosas				
N °	Procedimiento de restauración	Responsable	Tiempo límite de ejecución	Aprobador
1	Identificar las comunicaciones que están realizando conexiones maliciosas en la red corporativa.	Desarrollador 1	3 horas	Analista de calidad
2	En caso estas comunicaciones no hayan sido bloqueadas, se debe realizar el bloqueo de estas en las plataformas de seguridad.	Desarrollador 2	1 hora	Analista de calidad

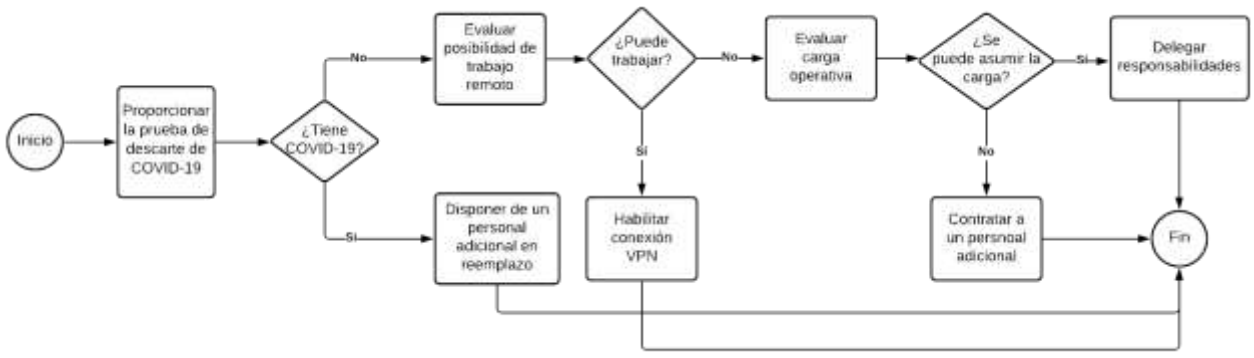
Conexiones maliciosas				
N °	Procedimiento de restauración	Responsable	Tiempo límite de ejecución	Aprobador
3	Evaluar la necesidad de potenciar la seguridad interna o perimetral.	Desarrollador 1	2 horas	Analista de calidad
4	En caso exista necesidad de adquisición de una solución de seguridad, se debe gestionar su compra.	Analista de RRHH	4 horas	Gerente General
5	Configurar la solución de seguridad adquirida	Desarrollador 1	3 horas	Analista de calidad



Flujograma 4. Procedimiento Conexiones maliciosas

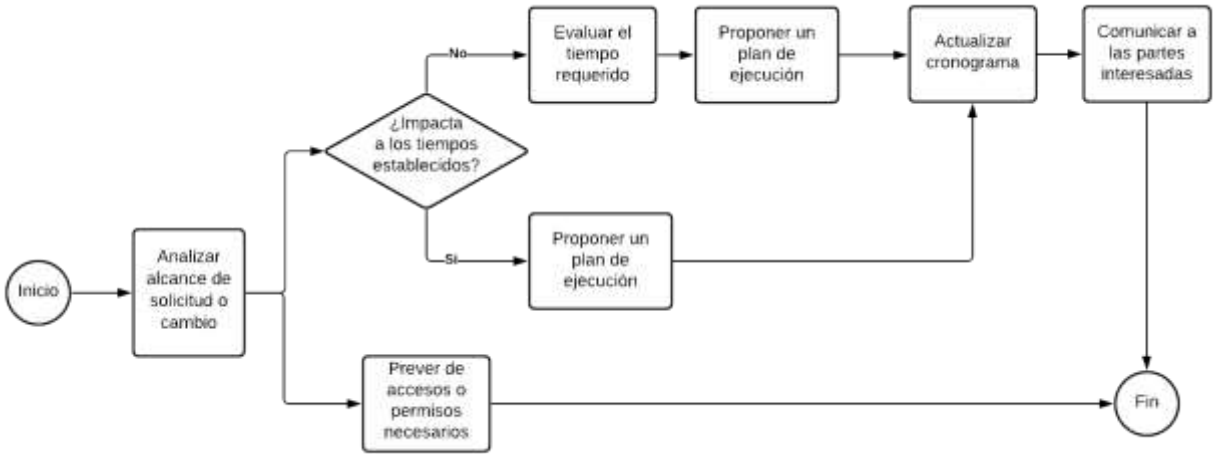
Enfermedades

N °	Procedimiento de restauración	Responsable	Tiempo límite de ejecución	Aprobador
1	Proporcionar al afectado la prueba de descarte para COVID-19	Analista de RRHH	1 hora	Gerente General
2	En caso no cuente con COVID-19, evaluar la posibilidad de trabajo remoto.	Analista de RRHH	8 horas	Gerente General
3	En caso pueda trabajar de manera remota, habilitar conexión VPN para el trabajo remoto. Caso contrario, evaluar carga operativa.	Desarrollador 2	1 hora	Analista de calidad
4	En caso la carga sea poca, delegar las responsabilidades. Caso contrario, contratar por honorario a un personal adicional.	Analista de RRHH	1 hora	Gerente General
5	En caso cuente con COVID-19, disponer de un personal adicional por un periodo de tres semanas como mínimo.	Analista de RRHH	8 horas	Gerente General



Flujograma 5. Procedimiento Enfermedades

Coordinación y planeación interna				
N °	Procedimiento de restauración	Responsable	Tiempo límite de ejecución	Aprobador
1	Analizar el alcance de la solicitud o cambio	Analista comercial	1 hora	Gerente general
2	En caso no impacte en los tiempos acordados, proponer un plan de ejecución.	Analista de calidad	3 horas	Gerente general
3	En caso de que impacte, evaluar tiempo que se requerirá y proponer plan de ejecución.	Analista de calidad	4 horas	Gerente general
4	Actualizar el cronograma de proyecto	Analista comercial	1 hora	Gerente general
5	Comunicar a las partes interesadas el cambio	Analista comercial	1 hora	Gerente general
6	Prever de accesos o permisos necesarios para posibles eventualidades.	Desarrollador 2	2 horas	Gerente general



Flujograma 6. Procedimiento Coordinación y planeación interna

12.10.6. Plan de recuperación frente a desastres

Se debe describir los procedimientos para recuperar los servicios en el sitio alterno de respaldo. Los siguientes procedimientos le ayudarán a recuperar los servicios en el sitio alterno. Se debe realizar cada procedimiento en la secuencia en que se presenta para mantener las operaciones eficientes. A continuación, se detallan las tareas necesarias para la recuperación frente a un desastre.

12.10.6.1. Traslado a la sede alternativa

Objetivos	
1	Evacuar sede principal
2	Movilizar al personal a la sede alternativa
3	Habilitar la conexión remota (VPN)

Criterios de activación	
1	Indisponibilidad para trabajar en la sede principal
2	Indisponibilidad para trabajar desde ubicación remota (aplica para empleados que realicen trabajo remoto)

N°	Subtareas	Responsable	Tiempo promedio de ejecución	Aprobador
1	Seguimiento y guía de evacuación del personal laborando físicamente en la sede	Analista de calidad	1/6 de hora	-

N°	Subtareas	Responsable	Tiempo promedio de ejecución	Aprobador
2	En caso sea necesario, aplicación de primeros auxilios.	Analista de RRHH	Inmediato	-
3	Coordinación y movilización del personal	Analista de calidad	1 hora	Gerente General
4	Confirmación de arribo a la sede alternativa	Analista de calidad	Inmediato	-
5	Evaluación de condiciones de trabajo	Analista de calidad	1 hora	Gerente General
6	Habilitación de conexión remota por VPN	Desarrollador 2	1 hora	Analista de calidad
7	Coordinación de movilización del personal en condiciones de realizar trabajo remoto desde casa	Analista de calidad	1 hora	Gerente General

12.10.6.2. Reactivación de procesos y servicios

Objetivos	
1	Activar tecnologías necesarias para reactivación de procesos
2	Reactivar procesos necesarios para continuar brindando servicios
3	Mantener en comunicación a todos los involucrados

Criterios de activación

Criterios de activación	
1	Fallas eléctricas en la ubicación física que comprometa operatividad
2	Traslado para trabajar desde la sede alternativa o desde remoto (casa)

N°	Subtareas	Responsable	Tiempo promedio de ejecución	Aprobador
1	Habilitación de conexión remota por VPN	Desarrollador 2	1 hora	Analista de calidad
2	Confirmación de accesos a los distintos servicios necesarios para la operación	Analista de calidad	Inmediata	-
3	Evaluación de cumplimiento de rutina de actividades diarias.	Analista de calidad	1 hora	Gerente General
4	Establecer medios de comunicación inmediata para los trabajadores	Desarrollador 2	1 hora	Analista de calidad
5	Comunicar a los clientes y trabajadores la total operatividad	Analista de RRHH	2 horas	Gerente General
6	Seguimiento del correcto funcionamiento de los servicios y procesos	Analista de calidad	Permanente	-

12.10.7. Plan de comunicaciones frente a desastres

Se debe describir los procedimientos de comunicación que tendrán que efectuarse en caso ocurra un desastre a nivel interno y externo.

Dentro del plan se comunicaciones se tendrá que definir las partes interesadas internas (personal y áreas de la empresa) y externas (clientes, proveedores, etc.), las estrategias de comunicaciones de la empresa y la asignación de roles y responsables de las comunicaciones en los procesos.

12.10.7.1. Partes Interesadas

Es necesario identificar las partes interesadas tanto internas como externas que sean relevantes para el desarrollo del SGCN, así como sus necesidades y expectativas. A continuación, se detallarán las partes interesadas.

Partes interesadas para las comunicaciones internas		
N °	Responsable	Comunicación
1	Gerencia	Comunicar los impactos de los incidentes
2	Trabajadores	Comunicar las políticas de seguridad

Partes interesadas para las comunicaciones externas		
N °	Responsable	Comunicación
1	Clientes	Comunicar accidentes que afecten a los servicios que tienen contratados
2	Servicios de Emergencia	Comunicar accidentes donde puedan haber víctimas o que puedan representar un riesgo

Partes interesadas para las comunicaciones externas		
N °	Responsable	Comunicación
3	Familiares de trabajadores	Comunicar accidentes o situaciones de salud que estén afectando a los trabajadores
4	Medios de comunicación	Comunicar accidentes que afecten a ciudadanos
5	Proveedores	Comunicar fallas de servicios o interrupción de servicios

12.10.7.2. Flujo de comunicación

En el flujo de comunicación se definirá como se realizarán las comunicaciones. De esta manera, podremos entender quién será el emisor, el destinario, cuál será el contenido del mensaje y los medios de comunicación para cada proceso. A continuación, se especificará el flujo de comunicación interno establecido en el Plan.

N°	Emisor	Mensaje	Receptor	Medio
1	Gerencia	Difusión de las políticas de continuidad de negocio	Todos los interesados, tanto internos como externos	Correo electrónico, telefónico y/o capacitación
2	Responsable del área afectada	Incidentes que requieren de asistencia externa	Proveedores	Correo electrónico o telefónico

N°	Emisor	Mensaje	Receptor	Medio
3	Persona o responsable del que detecta el incidente	Incidentes que pueden afectar la continuidad del negocio	Gerencia y responsable de la continuidad	Personal o telefónico
4	Recursos humanos	Incidente que afecta la integridad de los trabajadores	Familia del trabajador	Telefónico
5	Responsable de continuidad	Reportes del estado de la continuidad del negocio	Gerencia	Presentación
7	Responsable de continuidad	Informes de auditoría ISO 22301	Gerencia	Presentación
8	Responsable de continuidad	Informe de BIA e informe de análisis de riesgos	Gerencia	Presentación
10	Responsable del BCP	Informes de pruebas del BCP	Involucrados en las pruebas	Correo electrónico
12	Responsable del BCP	Modificaciones del Plan de Comunicaciones Frente a Desastres	Todos los involucrados	Correo electrónico

12.10.8. Plan de Pruebas

El plan de pruebas es la etapa en la cual se determinará la efectividad de los procedimientos implantados que son utilizados para responder una interrupción de las operaciones. Para elaborar el plan será necesario definir el alcance de las pruebas, las fechas de realización de pruebas, los requisitos previos para iniciar las pruebas, los roles y responsables de la realización de las pruebas y el detalle de las pruebas realizadas.

12.10.8.1. Planificación de pruebas

Se detallará el plan de pruebas a realizar para determinar la efectividad de los planes. Para llevar a cabo las pruebas, se definirán tres tipos de pruebas, así como niveles de responsabilidad para cada uno de estos. Para esto, se utilizarán los siguientes tipos de pruebas:

- Prueba Básica: Este tipo de pruebas serán llevadas a cabo en ambientes controlados como sala de reuniones donde se realizarán simulaciones de los posibles escenarios disruptivos.
- Prueba Intermedia: Este tipo de pruebas serán llevada a cabo en ambientes reales, donde sin hacer uso completo de los recursos, se realizará una simulación de un escenario disruptivo, donde también se verán involucrados los roles que son relevantes dentro del plan correspondiente.
- Prueba Completa: En este tipo de pruebas se realizará una simulación donde se realizará la activación de los procedimientos definidos en el plan correspondiente, se utilizarán los recursos definidos para el escenario disruptivo y serán involucrados todos los participantes.

Por otro lado, con respecto al nivel de responsabilidad de los trabajadores dentro de los planes del SGCN, se tendrá que definir los niveles de responsabilidad

- Nivel 1: Informado, recibe avisos y notificaciones.
- Nivel 2: Asignado para coordinaciones con actividades de despacho, llamadas y responder correos.

- Nivel 3: Participación constante durante la ejecución de pruebas.

Planes								
N°	Fecha	Plan	Tipo de Prueba	Nivel de Responsabilidad				
				Gerencia	Desarrollo	RRHH	Comercial	Clientes
1	Diciembre 2020	BCP	Prueba Básica	1	2	2	2	
2	Enero 2021	DRP	Prueba Intermedia	1	3	2	3	1
3	Febrero 2021	Plan de Comunicaciones	Prueba Básica	1	2	2	2	
4	Abril 2021	BCP	Prueba Intermedia	1	3	2	3	1
5	Mayo 2021	DRP	Prueba Completa	3	3	3	3	2
6	Junio 2021	Plan de Comunicaciones	Prueba Intermedia	1	3	2	3	1
7	Agosto 2021	BCP	Prueba Completa	3	3	3	3	2

Por último, al término de las pruebas, se tendrá que documentar los resultados obtenidos con el fin de determinar si los planes son eficaces.

Resultado de las pruebas sobre los planes						
N°	Planes	Duración Estimada	Día de inicio	Día de fin	Duración Real	Resultados
1	BCP	2 días	7/12/2020	9/12/2020	-	
2	DRP	1 día	4/01/2021	5/01/2021	-	
3	Plan de Comunicaciones	1 día	1/02/2021	2/02/2021	-	
4	BCP	2 días	5/04/2021	7/04/2021	-	
5	DRP	1 día	3/05/2021	04/05/2021	-	
6	Plan de comunicaciones	1 día	7/06/2021	8/06/2021	-	
7	BCP	3 días	2/08/2021	5/08/2021	-	

12.10.9. Mantenimiento

12.10.9.1. Mantenimiento de actividades

Se debe identificar las actividades de mantenimiento relacionadas con el Plan de Continuidad del Negocio:

- Revisiones periódicas
- Auditorías
- Modificación y/o ampliación tras simulacros
- Mejora de procesos internos tras resultados

A continuación, se detallan los elementos del Sistema de Gestión de Continuidad del Negocio que requerirán mantenimientos:

- Plan de negocio
- Documentación de comité de gestión de riesgos
- Matriz RACI
- Cronograma de concientización
- Análisis de Impacto al Negocio (BIA)
- Análisis de riesgos
- Matriz de requerimiento de recursos
- Plan de continuidad del negocio

Todos los puntos anteriormente mencionados, conforman la documentación necesaria para el Sistema de Gestión de Continuidad del Negocio, por ello se debe dar mantenimiento de forma anual.

Por otra parte, existe documentación propia de la empresa que permite la contextualización de los auditores, y por ende debe estar actualizada de acuerdo a la frecuencia de cambios organizacionales.

- Lista de inventario
- Lista de contactos

- Estándar de Procedimientos Operativos
- Procesos de negocios
- Documentación técnica

12.10.9.2. Mantenimiento de documentación empresarial

Se le debe dar mantenimiento a la documentación de la empresa de forma anual y con tres meses de anterioridad a la siguiente iteración del Sistema de Gestión de continuidad del Negocio.

12.11. Entregable 11: Checklist del control de Cumplimiento del Sistema de Gestión de Continuidad del Negocio (SGCN)

Desarrollo A1	Fecha: 11/11/2020
Puntos chequeados: ☐1 ☐ 2 ☒X ☐3 ☐ 4 5	Inspector: Analista Comercial

1. Documentación	
Plan de negocio empresarial	☒ SI ☐ NO
Acta de constitución	☒ SI ☐ NO
Acta de reunión definición de riesgos	☒ SI ☐ NO
Matriz RACI	☒ SI ☐ NO
Cronograma de concientización	☒ SI ☐ NO
Matriz de Análisis de Impacto al Negocio	☒ SI ☐ NO
Matriz de Análisis de Riesgos	☒ SI ☐ NO
Matriz de Medidas de Control	☒ SI ☐ NO
Matriz de requerimiento de recursos	☒ SI ☐ NO
Plan de continuidad	☒ SI ☐ NO

2. Gestión de Riesgos	
Criterios de evaluación del BIA definidos	☒ SI ☐ NO
Selección de actividades críticas	☒ SI ☐ NO
Definición de criterios de impacto en el análisis de riesgo	☒ SI ☐ NO
Definición de criterios de impacto en el análisis de riesgo	☒ SI ☐ NO
Evaluación de riesgos	☒ SI ☐ NO
Definición de estrategias	☒ SI ☐ NO
Definición de medidas de control	☒ SI ☐ NO

3. Actividades	
Actividades de concientización	☐ SI ☒ NO
Capacitaciones	☐ SI ☒ NO

4. Simulacros	
Pruebas de ejecución de plan de plan de continuidad del negocio	☐ SI ☒ NO

Pruebas de ejecución de plan de plan de recuperación frente a desastres	☐ SI ☒ NO
Pruebas de ejecución de plan de plan de comunicación frente a desastres	☐ SI ☒ NO

5. Actualizaciones	
Mantenimiento y actualización de documentación empresarial	☐ SI ☒ NO
Mantenimiento y actualización del SGCN	☐ SI ☒ NO

Observaciones
Toda ejecución de actividades o actualizaciones corresponde al segundo ciclo de plan de continuidad.

12.12. Conclusiones y Recomendaciones

Considerando tanto la estructura como el desarrollo del presente proyecto enfocado a cumplir con los objetivos de este, se puede concluir lo siguiente:

El diseño de un Sistema de Gestión de Continuidad de negocio, orientado a pequeñas empresas del rubro de desarrollo y consultoría de software, y en consideración del alcance mínimo establecido, permite que todas las empresas del nicho puedan contar con un cimiento sólido para la implementación del sistema de acuerdo con el contexto de cada una.

Permite contar con un entendimiento organizacional que se vea reflejado en los objetivos de la empresa. Esto quiere decir que, al disponer y formalizar toda documentación necesaria para

contar con el contexto necesario para poder aplicar el sistema, se evidencia las falencias y carencias de esta para que puedan ser subsanadas.

Con el análisis de impacto al negocio (BIA) y posterior a ello el análisis de riesgo, permite contar con todas las consideraciones y priorizaciones necesarias para determinar los controles que sean necesarios para poder reducir la probabilidad e impacto de los riesgos. Esto es de vital importancia dado que la activación de cualquier de los planes de continuidad debido a la materialización de un riesgo conllevan a gastos que impacta a pequeñas empresas.

Al disponer del diseño del sistema de gestión de continuidad de negocio, el evaluar la eficacia de las acciones y planes propuestos permitirá, que, en una segunda iteración de mantenimiento de este, se vean reflejados los resultados con un mejor entendimiento e imagen de la organización.

13. Bibliografía

Alberto, A. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información* (Primera ed.). Colombia: Alfaomega.

BSI. (2016). *ISO 22301 Business Continuity Management.* Recuperado el 22 de 09 de 2019, de bsigroup.com: https://www.bsigroup.com/globalassets/Documents/iso-22301/resources/iso-22301-implementation-guide-2016.pdf

Bureau Veritas. (2017). *IBM Cloud Infrastructure as a Service (IaaS) - ISO 22301:2012.* Obtenido de https://www.ibm.com/downloads/cas/PRAMEAL1?mhsrc=ibmsearch_a&mhq=iso%2022301

Calderón, J. (03 de Junio de 2014). Mitos sobre la Continuidad. Perú. Obtenido de https://cioperu.pe/articulo/16059/mitos-sobre-la-continuidad/

CertiProf. (2018). En *ISO 22301 AUDITO / LEAD AUDITOR.* CERTIPROF.

Certiprof. (2018). ¿Por qué es importante ISO 22301 para su organización? En *ISO 22301 AUDITOR / LEAD AUDITOR (I22301A/LA)* (pág. 24). CERTIPROF.

CertiProf. (2018). Términos y Definiciones. En *ISO 22301 AUDITOR / LEAD AUDITOR* (pág. 69). CERTIPROF.

Deloitte. (25 de Febrero de 2017, párr. 2). *¿Qué es crisis?* Obtenido de Deloitte: https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/que-es-una-crisis.html#

Gonzáles, G. A. (2017). Plan de Continuidad del Negocio basado en servicios en la nube para el área de tecnología (Tesis de pregrado). Guatemala: Universidad Galileo. Obtenido de http://biblioteca.galileo.edu/tesario/bitstream/123456789/578/1/Tesis%20-%20Plan%20de%20continuidad%20del%20negocio%20basado%20en%20servicios%20en%20la%20nube%20para%20el%20area%20de%20tecnologia.pdf

INACAL. (2014). *NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2014.* Lima.

ISO. (2018). *ISO 31000:2018(en)*. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

ISOTools Excellence. (26 de Enero de 2017). *Blog especializado en Sistemas de Gestión*. Obtenido de https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Marquina, L. D. (Septiembre de 2013). Diseño de un Sistema de Gestión de Continuidad de Negocios (SGCN) para la Reniec bajo la óptica de la norma ISO/IEC 22301 (Tesis de pregrado). Lima, Perú: Pontífica Universidad Católica del Perú. Obtenido de http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/5110

Osiptel. (12 de 09 de 2019). *OSIPTEL comparó la calidad de los servicios que brindan las empresas operadoras*. Recuperado el 22 de 09 de 2019, de osiptel.gob.pe: https://www.osiptel.gob.pe/noticia/osiptel-comparo-calidad-servicios-brindan-eo

Presidencia de Consejo de Ministros. (2014). *LEY DEL SISTEMA NACIONAL DE GESTIÓN DEL RIESGO DE DESASTRES Y EL PLAN NACIONAL DE GESTIÓN DEL RIESGO DE DESASTRES – PLANAGERD 2014-2021 recuperado de "https://www.mef.gob.pe/contenidos/inv_publica/docs/eventos-taller/taller-internacional-03y04-julio-2014".* Lima.

SGS. (2018). MAYORÍA DE EMPRESAS PERUANAS NO ESTÁN PREPARADAS PARA ENFRENTAR RIESGOS EN SU NEGOCIO. *SGS*. Obtenido de https://www.sgs.pe/es-es/news/2018/03/continuidad-del-negocio

Tejeda, Á. M. (2020). Garantizar la continuidad de negocio ante el COVID-19. *KPMG Tendencias*.

14. Anexos

14.1. Glosario de términos

Para facilitar el entendimiento del proyecto de investigación, se definirán conceptos basados en el Sistema de Gestión de Continuidad del Negocio. Estos serán utilizados a lo largo del desarrollo del tema de investigación.

14.1.1. Activo de la Información

Según (Alberto, 2007, pág. 44) “Un activo es algo que tiene valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Por esta razón, los activos

necesitan tener protección para asegurar una correcta operación del negocio y una continuidad en las operaciones". Por ello, un activo de la información, vendría a ser algo a lo que una organización le asigna un valor.

14.1.2. Probabilidad

La probabilidad es un término utilizado para referirse a la posibilidad de que un evento suceda., y que puede ser definido, mesurable o determino subjetiva u objetivamente, cualificable o cuantificable, y descrito usando términos generales o matemáticamente (como una probabilidad o frecuencia brindando un periodo de tiempo). (ISO, 2018)

14.1.3. Impacto

Se refiere a la consecuencia de la materialización de un evento que puede afectar de forma positiva o negativa y directa o indirectamente a los objetivos de la organización. El impacto puede expresarse de forma cuantitativa o cualitativa, y los efectos de este pueden escalar e ir acumulándose. (ISO, 2018)

14.1.4. Riesgo

El riesgo es el resultado de la probabilidad de que un evento ocurra por el impacto que este pueda tener en la organización. La ISO 31000 define este como "el efecto de incertidumbre en sobre los objetivos" (ISO, 2018). Los riesgos pueden ser positivos, cuando brinda oportunidades a la organización, y negativos, cuando la situación amenaza el cumplimiento de los objetivos de la organización.

14.1.5. Seguridad de la Información

La seguridad de la información se encarga de la implementación técnica de la protección de la información desde un punto de vista estratégico. Dentro de esta se tiene que tener en cuenta el análisis de riesgos, de las amenazas y de los posibles escenarios. Así mismo, tener en cuenta un marco normativo y de buenas prácticas, con el fin de mantener un nivel de confianza y madurez en la creación, utilización, almacenamiento, recuperación y disposición de la información. (ISOTools Excellence, 2017)

14.1.6. Seguridad Informática

La seguridad informática se basa en el cumplimiento de las políticas de seguridad y el análisis de riesgo en el que se debe basar dichas políticas. Del mismo modo, se encarga llevar a cabo la toma de medidas técnicas para la protección de los activos informáticos y de la información que se encuentra en medios digitales. (ISOTools Excellence, 2017)

14.1.7. Incidente de continuidad

Es un evento no esperado, el cual puede ser o puede ocasionar una interrupción de las actividades, operaciones, servicios o procesos, la pérdida de activos de valor y hasta dejar a la organización en estado de emergencia o crisis. (CertiProf, 2018, pág. 9)

14.1.8. Crisis

” Todos aquellos eventos inesperados e/o inevitables de carácter catastrófico que pueden afectar a los activos críticos, la estructura financiera, las personas e incluso la reputación, poniendo en peligro la propia supervivencia de la compañía.” (Deloitte, 2017, párr. 2)

14.1.9. Tiempo Máximo Aceptable de Interrupción (TMAI)

Es definido como el tiempo máximo en el que un producto o servicio a consecuencia de una interrupción puede estar inactivo, antes de transformarse en inaceptable. (CertiProf, 2018, pág. 6)

14.1.10. Objetivo Mínimo de Continuidad de Negocio (OMCN)

Nivel mínimo de servicios y/o productos que es aceptable por la organización para conseguir sus objetivos de negocio durante una interrupción. (CertiProf, 2018, pág. 69)

14.1.11. Resiliencia

Es la capacidad que prima en le gestión de continuidad de negocio, debido a que permite el continuo funcionamiento de la organización, luego de un incidente

reduciendo el impacto de la interrupción al mínimo hasta que la organización reanude sus servicios. (Certiprof, 2018, pág. 24)

14.1.12. Continuidad de Negocio y Operaciones

Capacidad de la organización para continuar brindando sus servicios y realizando sus actividades a niveles aceptables después de una interrupción. (CertiProf, 2018, pág. 9)

14.1.13. Plan de Continuidad de Negocio (BCP)

Procedimientos documentados que conducen a las organizaciones a responder, recuperar, reanudar y restaurar el nivel de operación predefinido después de una interrupción. (CertiProf, 2018, pág. 9)

14.1.14. Programa de Continuidad de Negocio

Proceso continuo de gestión y de gobierno, apoyado por la alta dirección y dotado de los recursos apropiados para implantar y mantener la gestión de continuidad del negocio. (CertiProf, 2018, pág. 9)

14.1.15. Instituto Internacional de Recuperación de Desastres (DRII)

Organización sin fines de lucro que ayuda a las organizaciones de todo el mundo a prepararse y recuperarse de los desastres proporcionando educación, acreditación y liderazgo de pensamiento en la continuidad del negocio y campos relacionados.

14.1.16. Instituto de Continuidad de Negocio (BCI)

Institución encargada de crear, divulgar y fomentar, a todos los niveles de la Sociedad, la cultura de la continuidad de negocio en su visión holística.

14.2. Matriz de consistencia

Problemática	Pregunta	Objetivo	Hipótesis
Dentro de las operaciones, servicios y actividades comunes de cualquier organización,	¿Cómo ayuda el diseño de un Sistema de Gestión de	Diseñar un Sistema de Gestión de la Continuidad del	El proyecto no contempla una hipótesis, debido a

siempre existen riesgos los cuales ponen en peligro el correcto funcionamiento y la continuidad del negocio.	Continuidad del Negocio basado en la norma ISO 22301 a la recuperación y mantenimiento de las actividades del negocio en niveles aceptables frente a un incidente o interrupción?	Negocio basado en la norma ISO 22301 para la rápida recuperación o el mantenimiento a un nivel aceptable de las actividades críticas del negocio frente a un incidente o interrupción.	que es de conocimiento general que la implementación de un SGCN basado en un estándar internacional traerá consecuencias positivas y facilitará el cumplimiento de los objetivos de la empresa. Por lo cual, este proyecto se enfocará en brindar el diseño de un SGCN con el fin de favorecer y agilizar el proceso de su implementación en empresas del rubro de consultoría y desarrollo de software.
El Perú en el año 2017 vivió desastres naturales que ocasionaron pérdidas, debido al calentamiento global y el	¿De qué manera entender la organización y sus necesidades	Entender a la organización y sus necesidades para establecer el contexto	-

fenómeno del niño. Por ello, muchas organizaciones y empresas de múltiples sectores dejaron de brindar de forma correcta e interrumpir por varios días sus servicios. Pese a conocer el contexto en el que se encuentran, existieron entidades del estado y entidades privadas que no cumplieron la ley que establece obligatorio el uso y ejecución de planes contra desastres, y la ejecución de obras que se debieron cumplir para mitigar los efectos de los desastres naturales que año a año se viven en el país.	minimiza los riesgos a sufrir interrupciones que conlleven a una crisis?	en el que se aplicará el Sistema de Gestión de Continuidad del Negocio.	
En lo que va del año 2019, en el Perú se presentaron un total de 8043 interrupciones de servicios de telecomunicaciones, los cuales el 47% fueron por una mala gestión del almacenamiento de energía eléctrica, 27% por fallas en elementos de red, 13% por daños a la infraestructura causada por terceros producto	¿En qué medida las acciones a tomar en el SGCN van a cubrir las amenazas y oportunidades minimizan los riesgos negativos y maximizan los riesgos positivos en la organización?	Analizar las acciones a tomar para cubrir riesgos y oportunidades para el diseño del plan de continuidad en los procesos del Sistema de Gestión de Continuidad del Negocio.	-

de obras o fenómenos naturales, un 6% por vandalismo y un 4% por mantenimientos de parte de los operadores.			
Las empresas del rubro de consultoría y desarrollo de TI, también se vieron afectadas debido a la falta o mal establecimiento y ejecución de un plan de gestión de riesgos y de continuidad del negocio, esto deriva en pérdidas económicas, pérdida de clientes, incumplimiento de contratos, poca o nula fiabilidad de la calidad del proyecto, etc.	¿Cómo la evaluación de la eficacia de las acciones propuestas en el análisis de los riesgos del SGCN influye en la toma de decisiones?	Evaluar la eficacia de las acciones propuestas en el análisis de los riesgos del Sistema de Gestión de Continuidad del Negocio.	-

14.3. Matriz operacional

Variable	Definición	Dimensión	Indicador	Instrumentos
Diseño de Sistema de Gestión de la continuidad de negocio	Etapa que tiene como propósito brindar conocimientos de la situación actual de la	Entender la Organización	Realizar un Check-List	Check List
			Hacer Reuniones y lluvia de ideas	Acta de reunion
			Analizar el	BIA

	organización, así como analizar las carencias de esta.		impacto al negocio	
			Evaluar riesgos	Matriz de Riesgos
			Asignar roles y responsabilidades	RACI
			Gestionar Recursos	Check List
	Etapa en la que se definen las actividades acorde a las estrategias de continuidad, la revisión de la situación actual de la organización y definición de las principales amenazas y fortalezas.	Establecer Estrategias	Realizar el análisis FODA	FODA
	Etapa de apreciación de riesgos para poder establecer, implementar y mantener un proceso	Implementar Estrategias	Hacer las mejoras de la evaluación de riesgos	Matriz de Riesgos
			Hacer las mejoras al BIA	BIA
			Realizar la matriz	Análisis de brecha

	documentado para la evaluación de riesgo, del mismo modo se resume los requisitos necesarios para medir el rendimiento de la gestión de la continuidad del negocio		GAP	
			Proponer estrategia de respuestas	Matriz de Riesgos
			Determinar y seleccionar las estrategias	Matriz de Riesgos
			Establecer los recursos	Check List
			Establecer los planes para el SGCN	Planes para SGCN
			Realizar las pruebas y ejercicios	Check List
			Evaluar los procedimientos de continuidad de los planes del SGCN	Check List
			Realizar la auditoría interna	Auditoria
			Realizar el resumen ejecutivo	


U T P
Universidad
Tecnológica
del Perú